UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de una Red Privada Virtual basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Morales Chapman, Julio Armando (ORCID: 0000-0001-7857-255X)

Torres Leiva, Neyser (ORCID:0000-0001-6533-8879)

ASESOR:

Dr. Gamboa Cruzado, Javier Arturo (ORCID: 0000-0002-0461-4152)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de Servicio de Redes y Comunicaciones

TRUJILLO - PERÚ

2021

Dedicatoria

“A mi Madre, quien en todo momento me brinda su apoyo y motivación, lo que me permitió crecer en lo personal y profesional. A mi Tía Angélica y mis Abuelas Olga, Juana y Dora; por el gran cariño y amor brindado. A mi esposa, hijo, hermana, tíos y toda mi familia por su invalorable apoyo. “

Julio A. Morales Chapman

A mis Padres por haberme formado como la persona que soy en la actualidad; todos mis logros se los debo a ellos. Me formaron con reglas y con libertad, pero al final me motivaron constantemente a lograr mis objetivos.

Neyser Torres Leiva

Agradecimiento

A Dios por haberme dado la fuerza y salud que me permite continuar cumpliendo con mis objetivos. A mi Padre, que desde el cielo guía mis pasos.

A los docentes universitarios, que impactaron en mí, gracias por su apoyo incondicional, por su amistad y por ser grandes ejemplos a seguir.

Julio A. Morales Chapman

A Dios por darme salud y permitirme cumplir mis objetivos, a mis padres porque fueron la base fundamental de mi formación, por enseñarme a ser perseverante y a no rendirme, gracias por sus motivaciones y sus consejos constantes, pero aún más por ese amor incondicional que me han brindado.

Neyser Torres Leiva

Índice de Contenidos

Dedicatoria ii

Agradecimiento ii

Índice de contenidos vi

Índice de figuras viii

Resumen x

Abstract xi

I. INTRODUCCIÓN 1

II. MARCO TEÓRICO 7

III. METODOLOGÍA 17

3.1. Tipo y diseño de investigación 17

3.2. Variables y operacionalización 18

3.3. Población, muestra y muestreo 21

3.4. Técnicas e instrumentos de recolección de datos 21

3.5. Procedimientos 22

3.6. Método de análisis de datos 22

IV. RESULTADOS 24

4.1 Desarrollo de la variable independiente (La Solución): Aplicando la metodología PPDIOO 24

4.1.1. Fase de Preparación 24

4.1.1.1. Direccionamiento IP 24

4.1.1.2. Topología Lógica 26

4.1.1.3 Topología Física 26

4.1.2. Fase de Planificación 29

4.1.2.1. Análisis y requerimientos de servicio de comunicación: 29

4.1.3. Fase de Diseño 33

4.1.3.1 Planeamiento IP 34

4.1.3.2. Diseño lógico propuesto 35

4.1.3.4. Seguridad en la Red Privada Virtual Propuesto 36
4.1.3.5. Diseño físico propuesto 38
4.1.4. Fase de Implementación 39
4.1.4.1 Instalación de sistema operativo 39
4.1.5. Fase de Operación 45
4.1.6 Fase de Optimización 46
4.2. Resultados 47
4.3. Prueba de normalidad 48
4.4. Análisis de resultados 51
4.5. Contrastación de la hipótesis 56
V. DISCUSIÓN 65
VI. CONCLUSIONES 70
VII. RECOMENDACIONES 71
REFERENCIAS 72
ANEXOS 77

Índice de tablas

Tabla 1 30
Tabla 2 31
Tabla 3 31
Tabla 4 32
Tabla 5 32
Tabla 6 33
Tabla 7 35
Tabla 8 36
Tabla 9 38
Tabla 10 40
Tabla 11 41
Tabla 12 41
Tabla 13 42
Tabla 14 42
Tabla 15 43
Tabla 16 43
Tabla 17 45
Tabla 18 45
Tabla 19 46
Tabla 20 47
Tabla 21 61
Tabla 22 65
Tabla 23 66
Tabla 24 68
Tabla 25 69
Tabla 26 70

Tabla 27 71
Tabla 28 73
Tabla 29 75
Tabla 30 77
Tabla 31 91
Tabla 32 92
Tabla 33 93

Índice de figuras

Figura 1 16
Figura 2 28
Figura 3 37
Figura 4 38
Figura 5 39
Figura 6 44
Figura 7 46
Figura 8 48
Figura 9 49
Figura 10 50
Figura 11 51
Figura 12 52
Figura 13 53
Figura 14 53
Figura 15 54
Figura 16 54
Figura 17 55
Figura 18 56
Figura 19 56
Figura 20 57
Figura 21 58
Figura 22 59
Figura 23 59
Figura 24 60
Figura 25 62
Figura 26 72

Figura 27 64
Figura 28 72
Figura 29 74
Figura 30 76
Figura 31 78
Figura 32 80
Figura 33 81
Figura 34 82

Resumen

Este proyecto como tal, es una propuesta de implementación de una Red Privada Virtual basada en la metodología PPDIOO, cuyo objetivo principal es mejorar la seguridad informática en la red de Lima Traylers S.A.C. Esto conlleva a múltiples objetivos específicos, tales como mejorar la cantidad de incidencias, controlar la cantidad de usuarios conectados en la red, disminuir el tiempo para acceder a las carpetas compartidas y mejorar el nivel de satisfacción de los usuarios.

Se consideró como muestra significativa a 30 procesos que involucran la seguridad informática en la red de Lima Traylers S.A.C.; asimismo para el análisis y recolección de información se utilizó fichas de observación. Además, tuvo enfoque cuantitativo y su diseño fue experimental puro; para contrastación de las hipótesis se aplicó la prueba estadística paramétrica t de Student para los datos que tuvieron un comportamiento normal y también se aplicó la prueba de U Mann-Whitney para los datos que no tuvieron un comportamiento normal.

Finalmente, los resultados que se obtuvieron en consecuencia del uso de la red privada virtual basado en la metodología PPDIOO en la seguridad informática de la red de Lima Traylers S.A.C., condujo al decremento de la cantidad de incidencias reportadas por los usuarios en un 76.7%, la reducción de la cantidad de usuarios conectados en la red en un 86.70%, también se redujo el tiempo para acceder a las carpetas compartidas en un 100%, y por último el nivel de satisfacción de los usuarios se aumentó en un 76,7% efectuando al cumplimiento de los objetivos de esta tesis.

Palabras clave: red privada virtual, vpn, openvpn, linux, usuarios.

Abstract

This project is a proposal for the implementation of a Virtual Private Network based on the PPDIOO methodology, which main objective is to improve computer security in the network of Lima Traylers S.A.C. This leads to multiple specific objectives, such as improving the number of incidents, controlling the number of users connected to the network, reducing the time to access to shared folders and improving the level of user satisfaction.

For this reason, this research pretends to present a solution using the OpenVPN suite under a free software platform, Linux operating system. In order to make this research more understandable, it has been divided into five chapters, the contents are as follows:

30 processes involving computer security in the Lima Traylers S.A.C network were considered as significant sample; also, observation files were used for the analysis and data collection. In addition, it had a quantitative approach and its design was pure experimental; to contrast the hypotheses, the Student t parametric statistical test was applied for the data that had a normal behavior and the U Mann-Whitney test was also applied for the data that did not have a normal behavior.

Finally, the results obtained in a sequence of the use of the virtual private network based on the PPDIOO methodology in the computer security of the Lima Traylers S.A.C. network, led to a decrease of 76.7% in the number of incidents reported by users, the reduction in the number of users connected to the network was 86.70%, the time to access to shared folders was also reduced by 100%, and finally the level of user satisfaction increased by 76.7% carrying out the fulfillment of the objectives of this thesis.

Keywords: virtual private network, vpn, openvpn, linux, users.

I. INTRODUCCIÓN

Realidad problemática.

Los últimos dos años el mundo ha sido impactado por una pandemia que ha realizado muchos cambios en la forma de vivir y laborar de cada uno de nosotros, las diversas empresas afectadas por la actual pandemia deben pensar en el trabajo remoto como una opción a la continuidad laboral, la digitalización de los negocios y con ello la toma de decisiones que permitan la subsistencia económica en las actuales circunstancias. Un gran número de decisiones de negocio pasan por evolucionar tecnológicamente, con ello maximizar la seguridad de la información es de vital importancia en la empresa. Por lo tanto, la mayoría de estas empresas necesitan el medio para sostener la comunicación rápida, segura y confiable donde quiera que sus oficinas se encuentren localizadas. Recientemente, la comunicación confiable ha implicado la utilización de líneas dedicadas para sostener una WAN (Red de área ancha). Esta última tiene enormes ventajas por encima de una red pública, por ejemplo; la confiabilidad, el funcionamiento y la seguridad. Aunque mantener una WAN, resulte ser costosa actualmente. Por otro lado, para las empresas, las líneas dedicadas no son una solución admisible, y se puede necesitar con frecuencia que los empleados se conecten a la red corporativa remotamente como se viene realizando actualmente, mediante el trabajo a distancia y así poder acceder a información sensible de la organización.

En la actualidad algunas empresas han crecido de forma desorganizada, dejando de lado las tecnologías de la información, por ende, la infraestructura de redes y comunicaciones, a medida que va creciendo se va viendo afectada, por las grandes cantidades de información que manejan y comparten día a día.

Sin embargo, en el Perú, según INEI el 21.9% de las empresas invirtieron en tecnología para sus comunicaciones, mientras que el 78.1% no lo hicieron, sobre todo en Lima donde se encuentra la mayor cantidad de empresas, habiendo crecido sin una planificación estratégica en su infraestructura de redes y comunicaciones, siendo una de ellas la empresa LIMA TRAYLERS S.A.C. que hasta la fecha no dispone de implementaciones de tecnologías de la información para potenciar la gestión de servicios y proyectos internos.

La fabricación de carrocerías en el Perú, se ha incrementado de manera importante últimamente debido a diversas necesidades del sector industria, minería, producción, transporte, entre otros sectores. La empresa ha implementado tecnologías de la información, pero con el pasar del tiempo se han vuelto obsoletas debido a la falta de atención y a la resistencia al cambio principalmente.

La inversión en la minería dentro del Perú es de gran presencia durante los últimos años, impulsando el avance de la industria nacional, que ahora compite al nivel más alto internacionalmente en producción de maquinaria para la minería e incluso, para los sectores como el de hidrocarburos y el pesquero.

Este avance se evidencia en el aumento del valor de exportación de los productos del sector metalmecánico. Durante los últimos seis años, los envíos en este sector han crecido a una tasa promedio anual del 21%. En 2008, cuando la economía mundial se vio duramente golpeada por la crisis financiera, registró el mayor crecimiento (+48%), luego se desaceleró a corto plazo en el 2011, para luego registrarse un aumento del 20.6% con respecto al año anterior. En el 2012 la tasa de crecimiento año tras año aumentaron un 12% las exportaciones, alcanzando los $545 millones de dólares. (Evolucióndel sector metalmecánico, 2013).

Raúl Berrios, CEO de RMB Sateci, empresa líder en el rubro, señala: Se considera que la industria nacional en carrocería está sobre los 200 millones de dólares manteniendo la industria dentro de la formalidad. Este año, con ventas superiores a los $ 20 millones, se mantiene el mercado con 35% en tolvas por lo general.

Berríos sostiene que la minería se reanudará en 2015 y un gran proyecto temporalmente paralizado se iniciará en 2014. “En los próximos años, mantendremos nuestra posición y lideraremos el mercado, desarrollando otras líneas de productos y exportando continuamente a Centroamérica y otros. países de la región. Y No solo exportar unidades, también exportar tecnología ". (Diario del País [en línea], 2014)

En estos tiempos, para que una industria sea competitiva en el mercado, logre más clientes y aumente su rendimiento, es necesario incrementar estrategias yponer en prácticas metodologías de mejoras que permitan el logro de estos objetivos. Es por esta razón que se sugiere implementar una red VPN site to site en la corporación Lima Traylers S.A.C. el cual permitirá mantener segura la información sensible, mediante software libre OpenVPN bajo sistema operativoLinux y así poder mantener una continuidad del negocio ante un ataque o vulnerabilidad a su seguridad informática.

Lima Traylers S.A.C. brinda el servicio de carga pesada y fabricación de carrocerías. La empresa se encuentra ubicada en la Avenida Alfredo Mendiola 8082 - Los Olivos, en la ciudad de Lima. El propietario y gerente general es el Señor Clemente Calderón Bueno; en esta empresa fabrican diferentes tipos decarrocerías, entre cisternas, furgón, plataforma y volquetes; sus principales clientes son las diversas empresas mineras, de transportes de cargas y la cervecería Backus. La empresa fue establecida en el año 2002 y actualmente tiene más de 100 trabajadores.

En la problemática están involucradas diferentes áreas y personas, desde el más alto mando quienes son los más preocupados por la continuación del negocio, entre los cuales forman parte el Gerente General, Presidente de Directorio, Administrador y el Jefe de Almacén; quien se encarga de manejar los pedidos y los inventarios; así como el Jefe de Compras; quien analiza los pedidos y determina la compra a los proveedores según los presupuestos, el Jefe de Operaciones; quien debe llevar el control de las operaciones del negocio, así mismo el Jefe de Ingeniería, quien se encarga del diseño y fabricación; y el área de la alta gerencia encargada de la gestión, administración, selección depersonal, monitoreo de todas la áreas y procesos.

Al encontrarse alejados geográficamente al tener su planta principal en la región de Lima, donde la sucursal principal está ubicada en San Martín de Porres y dos sucursales adicionales una en el distrito de Comas y otra en la región Callao, distrito Callao; las antes descritas no cuentan con una red privada que le permita distribuir información, obteniendo como resultado incidencias reportadas por diferentes usuarios debido a cuestiones de demora e intermitencias en el servicio, siendo un promedio de 15a 20 incidentes por día;

se debe a la carencia de acceso a la información y la falencia operativa con el servicio de red o dispositivos (Router, Switch), ocasionando que la información no se encuentre disponible las 24 horas del día, afectando las decisiones del negocio.

La seguridad informática es inestable (contraseñas débiles, falta de respaldo dela información, inadecuado uso de dispositivos de almacenamiento), se debe aque el personal que está laborando desde sus hogares y se conecta mediante el internet sin ninguna medida de restricción, lo que ocasiona robo de la información.

Los dispositivos de red (2 Router y 6 Switch) están dispersos por las diferentes áreas de trabajo, se debe a que no cuentan con un data center en donde se puedan fijar, lo que ocasiona que los equipos de red estén en la intemperie y nocumplan con los estándares mínimos internacionales.

Para acceder o realizar algún proceso desde la computadora, los tiempos de carga son de 4 a 7 minutos, esto supone inconvenientes como: demora al recibir o enviar información a través de correo, ralentización en la carga de archivos e inventarios, retrasos al ingresar al sistema de compras, demora para el ingreso de evidencias del diseño y fabricación de carrocerías, afectando completamentela productividad del negocio.

Por lo tanto, con el fin de garantizar el tráfico de los datos y asegurar la información sensible, ajustando el grupo de reglas de la seguridad de información aplicando los protocolos correctos, se propone implementar una red VPN para la empresa Lima Traylers S.A.C, la cual permita potenciar su seguridadinformática en toda la red de la empresa, teniendo como base la ISO 27001 y CISCO el cual es un modelo empresarial (De La Cruz, y otros, 2019).

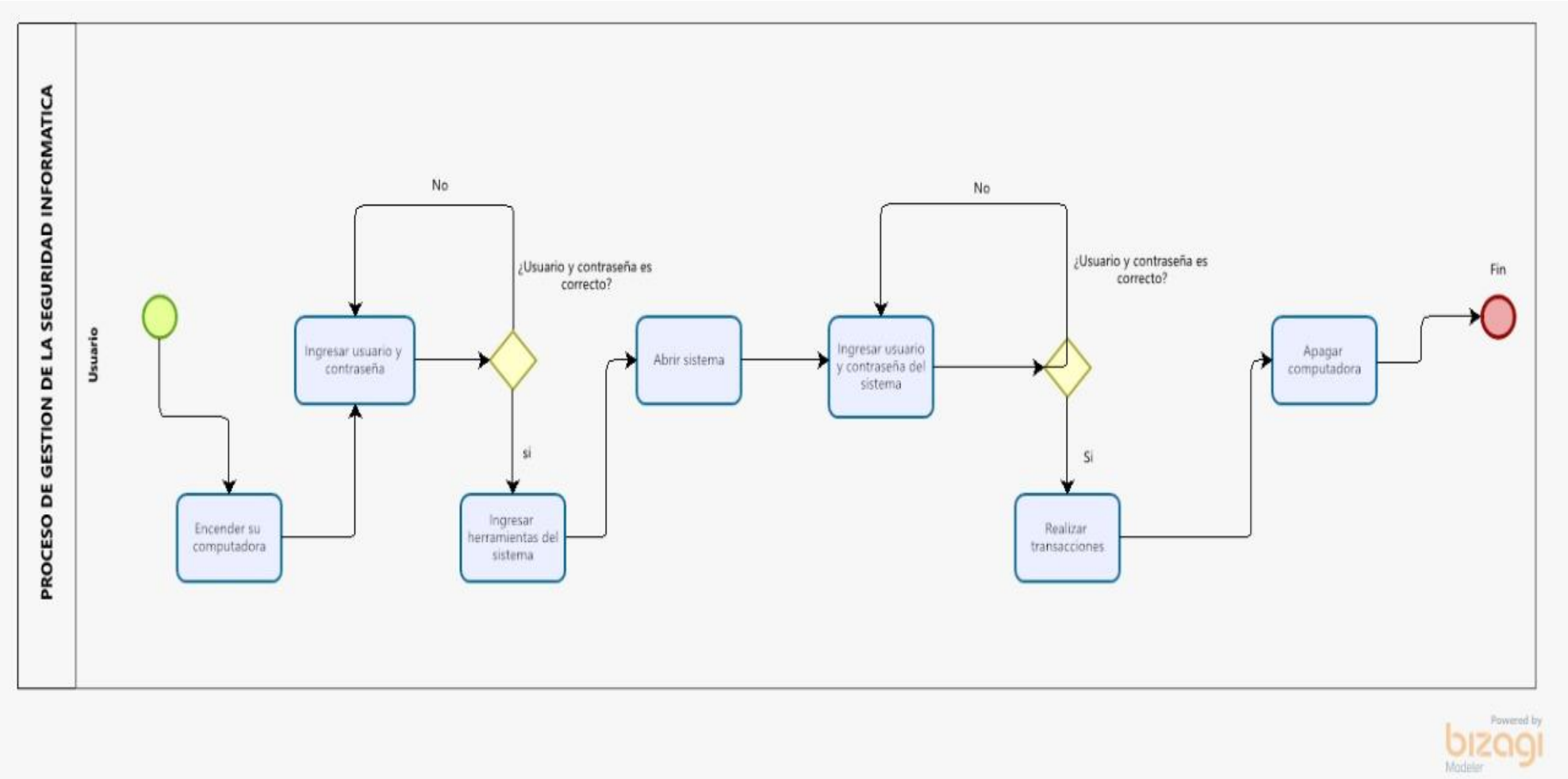


Figura 1: Proceso de seguridad informática en la empresa Lima Traylers S.A.C.

Indicadores.

a) Cantidad de incidencias reportadas por los usuarios. (Tacilla Ludeña, 2016)

b) Cantidad de usuarios conectados en la red. (Ramirez Varona, 2020)

c) Tiempo para acceder a las carpetas compartidas. (Espinoza Chipane, 2018)

d) Nivel de satisfacción de los usuarios en la red. (Sanchez, 2018)

Definiendo de tal manera, el siguiente **problema general**: ¿De qué manera el uso de una red privada virtual, basada en la metodología PPDIOO, mejora la seguridad informática en la red de la empresa Lima Traylers SAC?

A continuación los **problemas específicos**: ¿De qué manera la implementación de una red privada virtual, basada en la metodología PPDIOO, reduce la cantidad de incidencias reportadas por los usuarios?, ¿De qué manera la implementación de una red privada virtual, basada en la metodología PPDIOO, gestiona la cantidad de usuarios conectados en la red?, ¿De qué manera la implementación de una red privada virtual, basada en la metodología PPDIOO, reduce los tiempos de carga al acceder a las carpetas compartidas?, ¿De qué manera la implementación de una red privada virtual, basada en la metodología PPDIOO, mejora el nivel de satisfacción de los usuarios?.

En seguida, describimos la justificación de la presente investigación, se generará acceso remoto a través de una Red Privada Virtual (VPN), mediante la cual se brinda el acceso a la red interna con usuarioy contraseñas que es proporcionado por el personal encargado de la empresa, en donde los trabajadores cuentan con los permisos y puedan acceder a sus dispositivos de oficina y gestionar sus estaciones de trabajo estando fuera de la empresa. Además, se emplearán diferentes tipos de niveles de autenticación como son, las llaves de autenticación o las credenciales de acceso para accedera la red privada virtual y así poder validar la identidad del usuario. La finalidad de la investigación es mejorar la confidencialidad del intercambio de la información que los empleados realizan día a día en sus labores cotidianas.

Se describe el objetivo general es mejorar la seguridad informática de la red en la empresa Lima Traylers S.A.C, mediante la implementación de una red privada virtual basada en la metodología PPDIOO. A continuación, mencionamos los objetivos específicos de la investigación **OE1.** Reducir el número de incidencias reportadas por los usuarios. **OE2.** Gestionar la cantidad de usuarios conectados en la red. **OE3.** Reducir los tiempos para acceder a las carpetas compartidas. **OE4.** Mejorar la satisfacción de los usuarios.

Se menciona la hipótesis de la investigación, la implementación de una red virtual privada basada en la metodología PPDIOO mejora significativamente la seguridad informática en la red de Lima Traylers S.A.C. Las hipótesis especificas son: La implementación de una red virtual privada basada en la metodología PPDIOO reduce el número de incidencias reportadas por los usuarios en la red de Lima Traylers S.A.C., La implementación de una red virtual privada basada en la metodología PPDIOO gestiona la cantidad de usuarios conectados en la red de Lima Traylers S.A.C., La implementación de una red virtual privada basada en la metodología PPDIOO reduce el tiempo de carga a las carpetas compartidas de Lima Traylers S.A.C., La implementación de una red virtual privada basada en la metodología PPDIOO mejora la satisfacción de los usuarios de Lima Traylers S.A.C.

II. MARCO TEÓRICO

A continuación, se mencionan referencias y antecedentes que sirven para guiarnos en el tema a abordar y garantiza la investigación mediante argumentos sólidos y buenas bases.

En primer lugar, conceptualizamos el significado de una red privada virtual (VPN la cual son sus siglas en inglés) como una comunicación entre usuarios y hosts que están geográficamente distribuidos en múltiples ubicaciones y administrados por la misma empresa. Esto también permite la separación de redesfísicas en diferentes redes virtuales. En cambio, las redes privadas garantizan entre hosts de redes virtuales la incorporación de la protección de datos, lo que permite conexiones

seguras dentro de una red. Obteniendo privacidad y confidencialidad, las redes privadas pueden atravesar por redes poco confiables y también comparten redes físicas con segmentos o partes que no confiables (Ramírez Páez, 2018).

Con respecto a la VPN hay un tipo que se adapta al modelo empresarial de Lima Traylers que es sitio a sitio por ser frecuentemente utilizadas por empresas con múltiples oficinas en diferentes ubicaciones geográficas que necesitan acceder y usar la red corporativa de forma continua. Con una VPN de sitio a sitio, una empresa puede conectar de forma segura su red corporativa con sus oficinas remotas para comunicarse y compartir recursos con ellas como una sola red (Network, 2020).

Para la cual se plantea solucionar la seguridad informática en la red de la organización, para eso tenemos se define como seguridad informática para el proceso de prevención y detección del uso no autorizado de sistemas informáticos. Implica el proceso de prevenir, detectar y por ende evitar que los intrusos utilicen sus recursos de TI de manera maliciosa con el fin de lucrar. (Valencia, 2020).

Se presenta una investigación internacional como la de (Pomar, 2019), quien determina el objetivo principal de implementar un método de que permita la conexión entre los empleados de la empresa y los proveedores. Para esto se hizo un estudio precio para identificar las diferentes necesidades los usuarios y proponer soluciones estratégicas. Pomar, eligió aplicar OpenVPN después de comparar todas las VPN. Esto se debe a que OpenVPN es un software gratuito y cumple con todos los requisitos comerciales sin costo adicional. En definitiva, la implementación de una red privada virtual que incluye software libre ha permitido a la empresa adaptarse para que todos los empleados solo puedan acceder a ella de forma remota únicamente con conexión a internet.

Adicionando la misma propuesta desarrollada en la tesis (Peña, 2016), en la cual consiste en diseñar e implementar una Red Privada Virtual utilizando método de autenticación LDAP, para la obtención de resultados aplicó una técnica de observación documental y arqueo bibliográfico, ejecutándose cada una de las fases planificadas. En este proyecto se desarrolló la metodología de proyecto factible cumpliendo con las 5 fases definidas por el autor, concluyendo que una VPN

garantiza la integridad, confidencialidad y seguridad de los datos, y lo más importante permite a usuarios en oficinas geográficamente separadas, proveedores externos, clientes y trabajadores remotos conectarse desde cualquier lugar del planeta de forma segura. Además, se aseguró la continuidad del negocio.

Para (Cadena, y otros, 2015) en su proyecto sobre la implementación y diseño de una Red Privada Virtual bajo servidores Linux y su Análisis de Factibilidad" plantean diseñar una red VPN, utilizando Linux Open Source como lo es OpenVpn con la ventaja de optimizar costos por el hecho de que cuenta con licencia libre, es una herramienta sencilla de usar que solo solicita una autentificación para contar con su uso y a su vez se adapta al control de acceso que requiere su facultad.

En el ámbito **nacional** tenemos a (Sánchez, 2018), cuya investigación "Mejora de la gestión de la información de los servicios en la empresa Técnica Plástica SRL mediante la implementación de una VPN en una red corporativa", se aplicó el tipo de investigación aplicada se aplica en el contexto de la gestión de servicios de información por Técnica Plástica SRL mediante la implementación de VPN en redes corporativas y para recopilar los datos, utilizamos una tabla de observación simple como herramienta de recopilación de datos. Esto nos permitió usar la prueba de normalidad de Shapiro-Wilk para analizar una población de 10 trabajadores de oficina que apoyan diferentes regiones y muestrear el mismo número para cada área, a través de la herramienta IBM SPSS Statistics, asimismo, se tuvo un 95% de nivel de confianza. Como resultado, se denegaron 60% usuarios y se realizaron 90% mejoras de cumplimiento con respecto a la gestión de la información. Concluimos que las VPN corporativas apoyan la gestión de la información en la empresa de Técnico Plástica.

A su vez, en Cajamarca (Cueva, 2018) también se enfocó en el efecto de la implementación de la VPN en la gestión de información corporativa de Deyfor. Usando la encuesta como instrumento para recopilar los datos y para comprobar la ejecución del proceso antes y después de la implementación de las hojas de observación de VPN, la implementación de VPN se realiza en equipos enrutadores con características de cifrado basado en hardware. Dando por hecho, que la

implementación de VPN tiene un impacto significativo en la gestión de información empresarial Deyfor.

En Lambayeque, (De La Cruz, y otros, 2019) con la finalidad de comprobar la mejora de la gestión en aplicaciones de intranet para la Universidad Nacional Pedro Ruíz Gallo siendo ideal el uso de la VPN, evitaría todo el afán del trámite documentario. Aplicando un diseño cuasi experimental, y fundamentada en el estándar ISO 27001 y el modelo empresarial CISCO.

El modelo empresarial CISCO, es una arquitectura que separa la red dentro de la empresa en distintas áreas funcionales, las cuales se denominan como módulos. El modularidad se basa en la incorporación hacia la arquitectura, el cual permite la flexibilidad dentro del diseño de la red empresarial, para así facilitar su implementación y solución de adversidades presentadas. (CISCO, 2017)

Por lo tanto, una Red Virtual Privada (Virtual Private Network) confiere a los usuarios remotos poder conectarse de forma segura al trabajo, con una conexión a Internet, a la que no se puede acceder desde una red exterior. La VPN se puede usar para hacer una conexión, usualmente con algún cifrado, a través del Internet, mediante dos dispositivos, y enviar tráfico de red por medio de túneles. Los dispositivos remotos pueden ser teléfonos o tabletas, computadoras o incluso enrutadores para la red, de modo que todos los clientes de la red tengan acceso al sistema en la red protegida. (Simpson, 2019)

Variable Independiente: Red privada virtual

Se mencionan las bases teóricas de la **variable independiente**, que nos brinde una conceptualización apropiada de los términos que utilizaremos.

VPN se basa en una arquitectura de conexión de **punto a punto**, para crear una conexión, debe estar validado jerárquicamente entre el usuario y el servidor a través de un certificado SSL / TLS + RSA remoto. Permite diferentes tipos de enlaces de redes como es el IEEE 802.11 WIFI, Ethernet 802 y datos móviles.

El certificado de Capa de Conexiones Seguras (SSL), cuyo acrónimo es Secure Sockets Layer, se conoce como protocolo de seguridad que busca acreditación digital para establecer interacciones seguras por medio del Internet. Actualmente se encuentra sustituido por el protocolo TLS, conocido también como Transport Layer Security. (El Cifrado Web, 2018)

Las redes VPN son una tecnología de un uso común, en el cual existen diversas herramientas y protocolos que podemos usar para administrarla, tales como OpenVPN, herramienta de código abierto potente y flexible, que admite el protocolo de seguridad SSL / TLS (Castillo, 2020). Además de permitir conexiones encriptadas al enviar paquetes de información, es decir, cuando se interrumpe durante el transporte por Internet no se puede leer fácilmente, solo para llegar al destino, comenzó a considerarse un modelo de conexión, como un túnel seguro de internet. La cual está herramienta nos permita establecer conexiones con los recursos locales de su empresa desde otras ubicaciones. (Yonan, 2018).

A su vez, el software a implementar para este tipo de solución es Open VPN software libre de código abierto considerado un conjunto de reglas o protocolos de conexión para establecer conexiones VPN mediante túneles cifrados. La programaciónde esta aplicación está desarrollada en C, basándose en enlaces de tipo Transport Layer Security (TLS) y Secure Sockets Layer (SSL).

Para prevenir y proteger la información de interferencias no autorizadas en las redes corporativas se debe practicar las bases de la seguridad de la red. Esto añade seguridad a los dispositivos individuales; La seguridad de la red se basa en cómo se comunican los dispositivos entre sí, además de aplicar a través de una herramienta que se utiliza para prevenir la invasión ilegal dentro de una red. (networkworld, 2018)

La Norma ISO 27001 será tomado en cuenta para la implementación de la VPN, como una norma internacional de Seguridad de Información la cual se basa en tres pilares, los cuales son: la integridad, la confidencialidad, y la disponibilidad de información de una empresa y de los sistemas y aplicaciones que la abarcan. Así mismo la aplicación de la metodología de desarrollo Cisco, PPDIOO (Planificación

- Diseño - Implementación - Operación - Optimización) brinda los beneficios del diseño de red jerárquico en la infraestructura de la red facilitando que el diseño a futuro sea escalable.

Las principales ventajas de una VPN, tiene la capacidad de la integridad y confidencialidad de datos, en el cual la integridad de la información significa que un archivo o mensaje enviado ya no puede ser modificado. La confidencialidad se describe a que solamente los usuarios autorizados cuentan con acceso a información de la VPN. Además, se minimizan los costos y es fácil de usar. Facilitando enormemente la comunicación entre los diferentes tipos de usuarios realizando trabajo remoto. (Cisco, 2018)

Variable Dependiente: Seguridad Informática

De otra menara, se manifiestan las bases teóricas de la **variable dependiente**, en cual nos ayudará para conocer los términos de dicha variable.

La seguridad informática, se encarga de abordar y diseñar las normas, los procedimientos, técnicas y métodos con el objetivo de conseguir un sistema de información confiable, disponible y sobre todo seguro. Las principales tareas de seguridad informática, es poder minimizar los riesgos, en la entrada de información, en el transporte de la información, de los dispositivos que se utilizan para transmitir y recibir los paquetes de información, los diferentes tipos de usuarios y los protocolos que se usan para la implementación. Se clasifica en tres grupos: los usuarios, la información y la infraestructura. (Romero Castro, y otros, 2018).

El autor (Postigo Palacios, 2020); manifiesta que la seguridad informática de cualquier organización se ha convertido en uno de los pilares más sensibles y vulnerables, y se hace imprescindible la búsqueda de mecanismos para fortalecerla. El plan de seguridad se convierte en un instrumento primordial en el procesamiento de la información, en el aprovechamiento de los recursos tecnológicos y en el desarrollo de nuevas aplicaciones y tecnologías para la implantación de sistemas avanzados. Se mencionan las fases planificación de la seguridad informática,

servicios y mecanismos de seguridad, desarrollo de auditorías, permisos y derechos de usuarios, monitoreo del tráfico de red, ataques y test de intrusión y la auditoria de seguridad informática.

Continuando con la teoría relacionados al tema, los autores (García Cervigón, y otros, 2011), la seguridad informática es importante para las empresas, por lo que en pérdidas económicas y de tiempo podría suponer, una catástrofe, sin olvidarnos del peligro que podría ser el acceso no permitido a la red de un usuario no autorizado. Se considera vital la seguridad informática, como son un grupo de dispositivos, procedimientos y herramientas diseñadas para asegurar la privacidad, integridad y disponibilidad de información en una red informática, reduciendo lasamenazas que puedan afectar a la empresa.

Se menciona que el nivel de seguridad informática, se focaliza en proteger la información, la disponibilidad e integridad, la cual es de suma importancia para las diversas empresas con el fin de salvaguardar su información ante cibercriminales que puedan realizar daños. La confidencialidad, trata de asegurar que sólo los trabajadores autorizados accedan a la información que les corresponde. Se señalan sus tres recursos principales: gestión de privilegios, autenticación de usuarios, y cifrado de información. Asimismo, la integridad de la seguridad, consiste en salvaguardar que la información no se extravié, ni se comprometa de forma equivocada, se monitorea la red para encontrar posibles intrusos, revisar los sistemas de información y realizar copias de seguridad programadas que ayuden a tener la información en su estado anterior. La disponibilidad de la información, dispone de una seguridad que solo ciertos trabajadores puedan acceder a dicha información, se tiene que aplicar normas y procedimientos aplicados al uso de los sistemas de información ante probables ciber amenazas. (VERA NAVARRETE, 2018).

Los dispositivos son asignados de manera directa a una sección de la red, los dispositivos de los trabajadores se conectan a los dispositivos de una red, donde se posibilita su comunicación. Los tipos de dispositivos de red son: Router, Switch, Modem, Hub y Repetidor. (Lederkremer, 2019).

Definición de incidencias

Es todo suceso o imprevisto el cual tenga una relación directa o indirecta sobre la ejecución de sus actividades. El incorrecto diseño o la ejecución de uno o varios procesoso la falta de recursos establecidos pueden ser el origen de las incidencias

La gestión de incidencias, es un tema importante que todas las empresas deberían observar. Ya que su principal objetivo es de solucionar cualquier incidente que se presente de formaeficiente, ágil y eficaz realizando el análisis del cómo fue que ocurrió dicha incidencia y buscando se vuelva a repetir a futuro (Vásquez, 2019)

Clasificar las incidencias ayuda a los administradores de la red a indagar soluciones aplicables, registrar el flujo de trabajo y escalar dicha incidencia al siguiente nivel priorizando su atención.

Dentro de ellas, existen diversas incidencias externas que son las que se producen con proveedores y/o clientes, e incidencias internas las cuales se producen con los trabajadores de la empresa. (Vásquez, 2019).

Gestión de usuarios

(Ales, 2017) Los administradores de sistemas son los que realizan la atención a lososusuarios mediante la instauración de normas que regulen el uso de la red. No solo es administrar las cuentas de acceso al sistema o instalar un software en la PC del usuario.

Para que ambos interactúen de forma óptima es necesario el apoyo constante por parte del área de dirección de la empresa en la aplicación de estas normas, de manera que quede evidenciado cómo y cuándo deben notificar los usuarios los problemas de la red al administrador, así como solicitar que los trabajadores lleven a cabo una parte del trabajo para mejorar la gestión y cómo hacer un seguimiento de estos problemas y peticiones.

El usuario debe recibir el soporte que solicita, siempre que lo haga por las vías establecidas.

Todos los trabajadores deben ser tratados por el mismo patrón sin favoritismos.

El trabajador debe ser capacitado sobre algunos conocimientos técnicos de la red.

La formación a los trabajadores es uno de los elementos claves para reducir las incidencias.

Gestión de tiempo

(Salazar, 2017) El factor tiempo es vital en las empresas, ya que influye en todas las tareas y actividades que se efectúan para el cumplimiento de los resultados del negocio. Saber administrar los recursos del negocio es una forma de controlar el tiempo y alcanzar los objetivos. La adecuada gestión del tiempo se verá manifestada en las acciones y resultados que deben realizar los trabajadores, ellos se guían o se reflejan según el comportamiento de su jefe inmediato. De forma indirecta puede fortalecer las habilidades como directivo y como persona en todos sus trabajadores.

Criterios de almacenamiento.

Se elaborará ciertas reglas, una de ellas es que deba usarse la red corporativa siempre para la manipulación de la información, siendo una prioridad el uso de la VPN. Se debe considerar los siguientes aspectos: qué tipo de información debe o no debe almacenarse en los directorios de la empresa; que trabajadores tienen acceso a la información y si se modifica alguna condición de la información sea por actualización, modificación o cuándo sea necesario eliminar la información por demanda o por ya no ser de interés.

Nivel de satisfacción del usuario

El concepto de satisfacción del usuario se basa en la diferencia entre lo que los usuarios esperan y lo que perciben como un servicio. Por tanto, las percepciones subjetivas con expectativas previas forman una expresión de la calidad del servicio.

La satisfacción es un indicador de la calidad de la atención brindada por el servicio. Conocer su satisfacción lo ayuda a cerrar la brecha, redefinir sus fortalezas y desarrollar sistemas más eficientes que ofrecen mejor calidad a sus usuarios.

Variable Interviniente: Metodología PPDIOO

A continuación, se manifiesta la **variable interviniente**, en cual nos ayudó para conocer sus principales beneficios y fases de dicha metodología.

Metodología PPDIOO, es el desarrollo del ciclo de vida para el diseño e implementación de una red, formalizado por la empresa Cisco. Definiendo seis fases donde la letra inicial de la fase corresponde a sus siglas. Preparar, Planear, Diseñar, Implementar, Operar, Optimizar. (PPDIOO). Por consiguiente, selogra la optimización del desempeño de la red mediante su ciclo de vida.

Se detalla las fases de la metodología PPDIOO:

Preparación: Observar las necesidades para el desarrollo de un nuevo diseño de red de datos que pueda cubrir el propósito de la implementación de una VPN de acceso remoto.

Planeación: Identificar los requisitos y requerimientos que se necesitará la red. Mediante el análisis de la arquitectura, de los elementos, de los equipos que hay y los que se asume que harían falta.

Diseño: Desarrollar los requerimientos técnicos y de negocios mediante un diseño detallado, obtenido desde las fases previas. Se debe incluir diagramas de red y lista de equipos. La actualización del plan del proyecto se realiza con información detallada para ser tomada en cuenta en la implementación.

Implementación: Aplicar el trabajo realizado en las últimas tres fases a la par del desarrollo, los nuevos dispositivos se integrarán sin interrumpir las redes existentes ni crear agujeros de seguridad. Cada fase de ejecución contiene una descripción, pasos de implementación, detalles del tiempo de ejecución estimado y pasos para volver al escenario anterior en caso de error o falla.

Operación: Mantener la operatividad de la red diariamente 24/7 debe incluir la monitoreo y administración de los componentes de una red, el mantenimiento de ruteo, la administración en cuanto a actualizaciones, la administración del identificación, desempeño y corrección de errores de la red. Esta fase es la última prueba final del diseño.

Optimización: Administrar proactivamente, resolviendo e identificando cuestiones antes que alteren a la red. Se permite crear una transformación al diseño si surgen demasiados inconvenientes, para incrementar el desempeño o resolver cuestiones sobre las aplicaciones. (QUIDAN, 2020)

Entre otros factores positivos de la metodología PPDIOO, es aminorar el costo total de propiedad de la red, aumentar la disponibilidad de la red, mejorar la agilidad de la empresa y acelera el acceso a aplicaciones y servicios. (Sivasubramanian, y otros, 2010)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación: Aplicada.

Diseño de investigación: Experimental Puro

Figura 2. Diseño de investigación

Dónde:

R = *Elección Aleatoria de los elementos del Grupo.*

G_e = *Grupo experimental: Grupo de estudio al que se le aplicará la condición experimental (Red privada virtual).*

G_c = *Grupo de control: Grupo de control al que no se le aplicará la condición experimental (Red privada virtual).*

0_1 = *Datos de la PostPrueba para los indicadores de la VD: Mediciones PostPrueba del grupo experimental.*

0_2 = *Datos de la PostPrueba para los indicadores de la VD: Mediciones PostPrueba del grupo de control.*

X = *Red privada virtual: Condición experimental*

$--$ = *Falta la condición experimental.*

Se refiere a la creación de un grupo experimental (G_e) instituido por la implementación de una red privada virtual que mejora la seguridad informática, en el cual a los indicadores de Post-Prueba (0_1), se le administra el estímulo (X), para solucionar los problemas mencionados en el proceso, luego se espera los resultados deseados (0_2).

3.2. Variables y operacionalización

Variables

- **Variable independiente:** Red privada virtual.
- **Variable dependiente:** Seguridad informática en la red de Lima Traylers S.A.C
- **Variable interviniente:** Metodología PPDIOO

Indicadores

A. Conceptualización.

a) Variable independiente: Red privada virtual.

b) Variable dependiente: Seguridad informática.

Tabla 1. *Indicadores y conceptualización*

Cantidad de incidencias reportadas por los usuarios	El número de incidencias, son realizadas por los diferentes usuarios al momento de poder conectarse a la red de la empresa.
Cantidad de usuarios conectados a la red	Cantidad de usuarios que se conectan a la red mediante la VPN de la empresa.
Tiempo para acceder a las carpetas compartidas	Tiempo en segundos, en el cual el usuario demora al acceder a la información de las carpetas compartidas de la empresa.
Nivel de satisfacción de los usuarios en la red	Nivel de satisfacción de usuarios que necesitan acceder a la red de la empresa.

B. Operacionalización de variables.

a) Variable independiente: Red privada virtual.

Tabla 2*: Técnica de recolección de datos*

INDICADOR	ÌNDICE
Presencia Ausencia	No, si

b) Variable dependiente: Seguridad informática.

Tabla 3*. Indicadores de variable dependiente*

DIMENSIÓN	INDICADOR	ÍNDICE	UNIDAD DE MEDIDA	FÓRMULA	UNIDAD OBSERVACIÓN
Incidencias	Cantidad de incidencias reportadas por los usuarios	[1-2]	Incidencias / Día	----------	Observación indirecta
Seguridad	Cantidad de usuarios conectados a la red	[1-2]	Conexiones / Día	----------	Observación indirecta
Tiempo	Tiempo de carga al acceder a las carpetas compartidas	[30-0]	Segundos / Usuario	----------	Observación directa
Satisfacción	Nivel de satisfacción de los usuarios en la red	Totalmente de acuerdo, de acuerdo, ni acuerdo ni desacuerdo, en desacuerdo, totalmente en desacuerdo	Escala de Likert	----------	Observación indirecta

3.3. Población, muestra y muestreo

Según (Hernández, y otros, 2014), definen a una población como la agrupación de individuos los cuales cumplen con determinadas especificaciones.

Tabla 4*. Población y muestra*

Unidad Muestral	Procesos de la seguridad informática en la red. Restricciones: • Empresas de fabricación de carrocerías para tráilers. • Micro y pequeñas empresas alrededor del mundo
Universo	Todos los procesos de la seguridad informática de la red en micro y pequeñas empresas de carrocerías para tráilers. En vista que no se puede determinar el número de procesos antes mencionados, se tiene: N = Indeterminado
Muestra	Procesos de la seguridad informática de la red en la empresa Lima Traylers S.A.C. n = 30
Tipo de Muestra	Aleatorio

3.4. Técnicas e instrumentos de recolección de datos

Tabla 5*. Instrumento de recolección de datos*

INSTRUMENTO
• Ficha de observación

3.5. Procedimientos

Tabla 6. *Procedimientos*

PROCEDIMIENTOS
• Observación indirecta - Consulta base de datos - Consulta modem router - Ficha de observación

3.6. Método de análisis de datos

3.6.1. Etapas de análisis de resultados

1) Fase 1

Se selecciona un software adecuado para analizar los datos.

2) Fase 2

Se ejecuta programa MINITAB.

3) Fase 3

- Análisis de datos por indicador.
- Visualizar datos por indicador.

4) Fase 4

Se lleva a cabo el análisis estadístico descriptivo de cada indicador de estudio.

5) Fase 5

Se desarrolla los análisis estadísticos inferenciales con respecto a las hipótesis planteadas.

6) Fase 6

Se efectúan análisis adicionales.

7) Fase 7

Se preparan los resultados para su presentación.

3.6.2. Software de análisis de datos

En este proyecto se utilizará el software especializado de análisis de datos MINITAB.

3.6.3. Medidas de la estadística descriptiva

1) Distribución de frecuencias graficas.

a. Histogramas

b. Tipo pastel

c. Tabla de frecuencias

d. Los polígonos de frecuencias

2) Medidas de tendencia central

a. Moda

b. Mediana

c. Moda

3) Medidas de variabilidad

a. El rango

b. La desviación estándar o característica

c. Varianza

4) Otras estadísticas descriptivas

a. La asimetría

b. La curtosis

3.6.4. Análisis estadístico inferencial

Esta fase será utilizada para probar las hipótesis poblacionales y estimar los parámetros.

1) Nivel de significancia

El nivel de significancia de 0.05.

2) Prueba de hipótesis

- Análisis paramétrico con la prueba t de Student.
- Análisis no paramétrico con la prueba de U de Mann-whitney

3.7. Aspectos éticos

Para el desarrollo de esta investigación se tuvo en cuenta los siguientes aspectos éticos, según la Resolución de Consejo Universitario Nº 0126-2017/UCV.

Se distingue la dignidad humana, independientemente de su origen, condición social o económica, género u otros rasgos, donde los intereses humanos y el bienestar preceden a los intereses científicos y la autodeterminación se respeta como creencia cultural. (artículo 3).

Se realizó una contribución igualatoria de todos los participantes de la presente investigación, sin exclusión alguna (artículo 5).

En esta investigación se cumplió de forma rigurosa los requisitos éticos, legales y de seguridad, respetando todos los términos y condiciones establecidas en los diferentes proyectos de investigación (artículo 9).

Se respetó los derechos del autor de las fuentes de información, citadas con las normas ISO 690 (artículo 16).

IV. RESULTADOS

4.1. Implementación de la Red Privada Virtual: Aplicando la metodología PPDIOO

4.1.1. Fase de Preparación

4.1.1.1. Direccionamiento IP

Cantidad de dispositivos conectados en la sede Comas.

Tabla 7. *Dispositivos conectados y distribución de IP*

Dispositivos conectados	Dirección IP de clase C
PC Almacén	192.168.1.50
PC Operaciones	192.168.1.51
PC Asistente de operaciones	192.168.1.52
PC Diseño Y corte	192.168.1.53
Servidor de archivos	192.168.1.54
Servidor VPN	192.168.1.150
Grabador digital de cámaras	192.168.1.120

Repetidor digital de cámaras	192.168.1.121
Cámara exterior	192.168.1.122
Cámara vigilancia	192.168.1.123
Cámara Fabricación	192.168.1.124
Cámara oficina piso 2	192.168.1.125

Tabla 8*. Dispositivos conectados sede SMP.*

Dispositivos conectados	Direccionamiento IP clase C
PC Gerente general	192.168.0.50
PC Sub gerente General	192.168.0.51
PC Administración	192.168.0.52
PC Contabilidad	192.168.0.53
PC Asistente contabilidad	192.168.0.54
PC Finanzas	192.168.0.55
PC Gerente de ventas	192.168.0.56
PC Asistente de ventas	192.168.0.57
PC Gerente de Proyectos	192.168.0.58
PC Dibujo técnico 1	192.168.0.59
PC Dibujo técnico 2	192.168.0.56
PC secretaria	192.168.0.57
PC Logística	192.168.0.58
PC Seguridad en el trabajo	192.168.0.59
PC Administración	192.168.0.60
PC Gerente de transportes	192.168.0.61
PC Asistente de transportes	192.168.0.62
Impresora Administración	192.168.0.20
Impresora ingeniería	192.168.0.21
Grabador analógico de cámaras	192.168.0.120
Grabador digital de cámaras	192.168.0.121
Repetidor digital de cámaras	192.168.0.122
Cámara exterior 1	192.168.0.123

Cámara exterior 2	192.168.0.124
Cámara fabricación 1	192.168.0.125
Cámara corte y doblado	192.168.0.126

4.1.1.2. Topología Lógica

La topología de LAN es estrella porque los dispositivos estás conectados directamente al punto central. En este caso, se utiliza el módem Reuter del proveedor ISP de acceso a Internet y, inevitablemente, toda la comunicación se realiza a través de él. Los dispositivos no están directamente conectados entre sí.

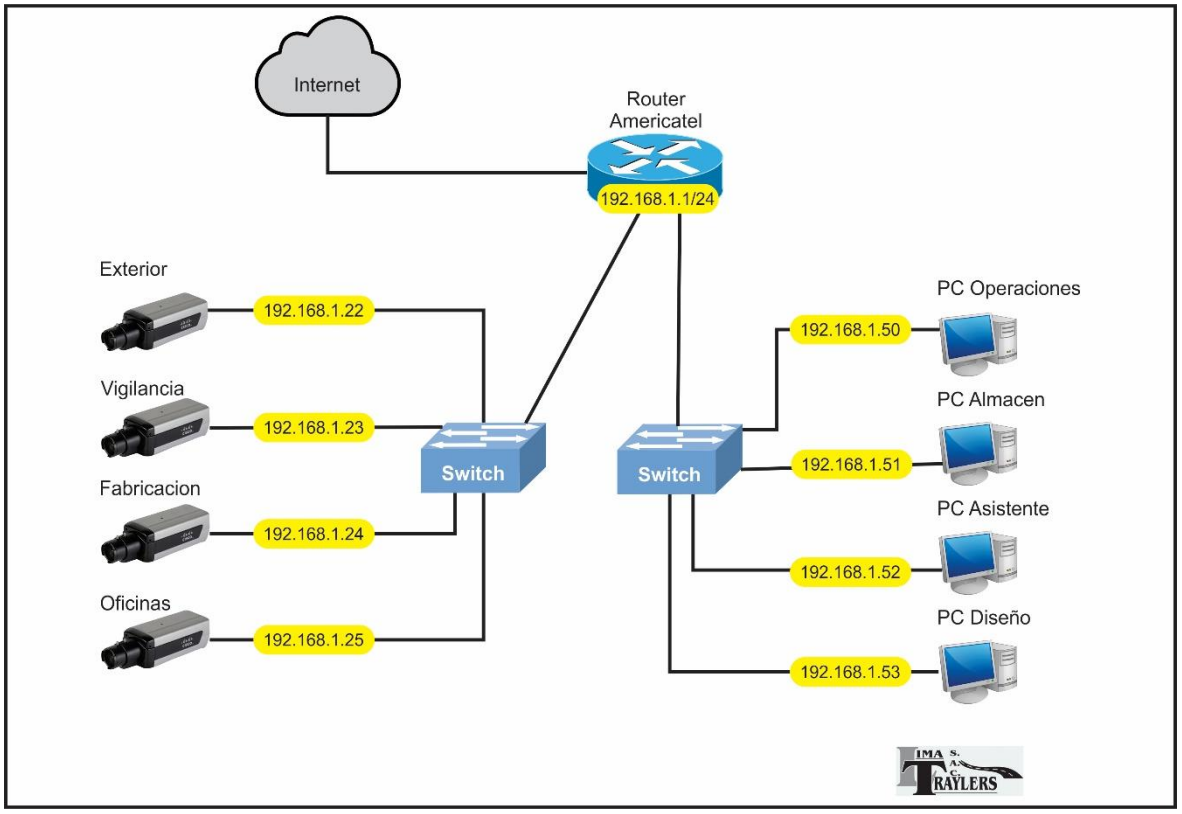


Figura 3. Topología lógica de red en estrella en relación a la conexión de sus terminales

4.1.1.3 Topología Física

Equipos interconectados: Modem Router Gaoke de tecnología antigua NGN (Next Generation Networking), esta red está basada en la trasmisión de paquetes capaz de trasmitir servicios integrados incluyendo teléfonos tradicionales.

Figura 4. Modem Router Gaoke

Cableado estructurado: Es un cableado estándar para Gigabit- Ethernet y algunos otros protocolos de red, la categoría es 6 y cuenta con certificación UL (Underwriters Laboratories). El estándar del cable proporciona un rendimiento para la trasmisión de datos de 1 gigabit por segundo, frecuencia de 250 MHZ. Este cumple en su totalidad con las normas eléctricas y de telecomunicaciones a nivel mundial, tales como TIA/ANSI/EIA 568C.2 e ISO/IEC 1 11801.

Tabla 9*. Especificaciones del cableado*

Ítem	Descripción
Normas internacionales	ANS/TIA/EIA-568-C.2 | ISO/IEC11801
Tipo de cableado	Par trenzado sin blindar
Marca y categoría de cableado	Nexxte solutions Cat. 6
Tecnología de cableado	Cobre UTP - 0 halógeno
Velocidad de trasmisión	1000 Mbps
Ancho de Banda	100 Mhz
Distancia máxima entre enlaces	90m

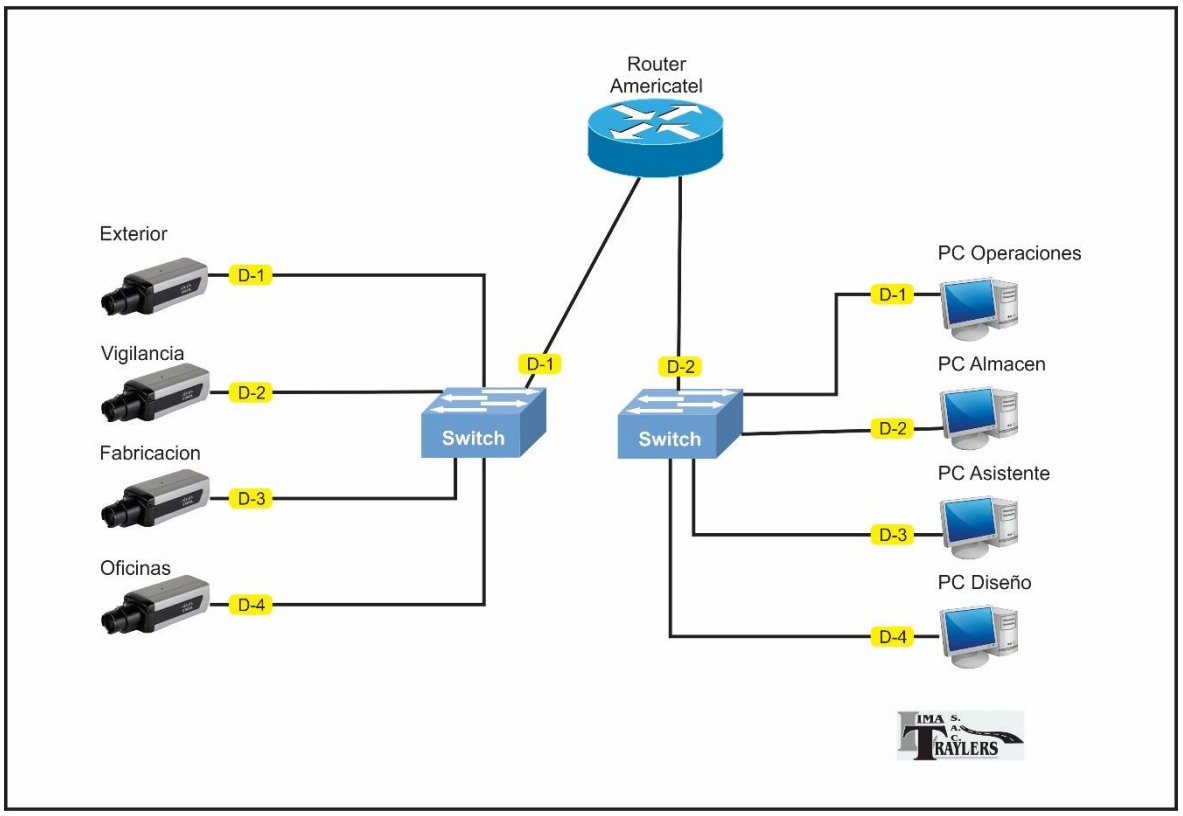


Figura 5. Topología física de red en estrella en relación a que se encuentran conectados las terminales

4.1.2. Fase de Planificación

4.1.2.1. Análisis y requerimientos de servicio de comunicación:

Luego de haber hecho un levantamiento de información realizado en la fase de preparación se necesita una serie de cambio para el rediseño a nivel de la capa 2, 3 y 4 de esta manera garantizar una mejora ante la cantidad de falencias y situaciones desfavorables que ocasionan bajo rendimiento en la seguridad informática, para ello se involucra los requerimientos, que me muestran a continuación.

Requerimientos de usuario final:

Para los requerimientos nivel usuario, se obtuvo la información mediante entrevistasa los usuarios y a la vez realizar encuestas formales con el fin de obtener una información real de la apreciación del usuario respecto al servicio de red y a la par que los usuarios establecen disponibilidad, seguridad y estabilidad en cuanto a los tiempos de respuesta.

Tabla 10*. Requerimientos de usuario*

Requerimiento	Objetivo
Conexiones estables	Enviar y recibir paquetes de información sin retrasos ni perdidas. Mejorar la comunicación entre nuestros dispositivos de red.
Disponibilidad para los usuarios	Acceder a la información cuando los usuarios lo requieran
Tiempo de acceso a los sistemas informáticos	Mejorar el tiempo para enviar y recibir email. Agilizar el tiempo de carga a los sistemas informáticos de la empresa

Requerimiento de Aplicación:

Para los requerimientos nivel aplicación implican él envió de correos, transferencia y acceso a los diversos sistemas informáticos, la conexión con estos servicios es importante. Como resultado tenemos la alta disponibilidad de red junto con la seguridad y priorización de tráfico, los cuales son requisitos primordiales para dichos servicios.

Tabla 11. *Requerimientos de aplicación*

Requerimiento	Objetivo
Integridad en la información	Hacer que la información se mantenga intacta, correcta sin ser modificada o manipulada por terceros mediante su trayecto.
Priorización de tráfico	Asegurar la priorización de tráfico y la garantía de un ancho de banda mínimo, priorizando paquetes en función de colas de prioridad.
Seguridad en la información	Controlar el acceso a las redes de datos con la intención de resguardar la información que es el activo más valioso de la empresa.

Requerimientos de infraestructura:

La infraestructura de una red debe ser escalable, que se pueda añadir nuevos componentes de forma continua y que funcione a la misma velocidad, confiable de contar con un hardware redundante, rápida de acuerdo a los estándares internacionales, disponible que se encuentre completamente activa cuando lo necesitemos.

Tabla 12. *Requerimientos de infraestructura*

Requerimiento	Objetivo
Flexibilidad	Permitir crecimiento de forma modular, y que se adapte a la nueva dinámica tecnológica, cada vez que las organizaciones necesiten implementar nuevas aplicaciones.
Administrable	Unificar los servicios en la red, controlar la carga de cada equipo, bloqueas o restringir el uso de equipos que generes problemas,

	optimizar el tráfico y mejorar la seguridad.
Confiable	Soportar aplicaciones robustas, funcionar a través de diferentes tipos de cables y dispositivos que compongan la infraestructura física.

Tabla 13*. Lista de equipos y accesorios para la implementación*

Nombre	Descripción
Servidor VPN Intel Core i5 10500 F	Sistema operativo Linux Ubuntu VMware para Linux
Accesorios de red	1 gabinete de pared 6 Ru Regleta Power 2 Patch-cord Cat 6. 1 bandeja de 1 RU
Switch TL-SG108	Velocidad de transferencia 10/100/1000Mbps Capacidad 8 puertos la Gigabit
Modem Router Empresarial	Accesos a red pública con puertos de comunicación Tecnología de comunicación NGN Por Radio enlace Ancho de banda de 2 Mbps.

4.1.2.2. Recurso humano designado para la implementación

Para el desarrollo de cada una de las fases de la metodología serán asignados los siguientes especialistas.

Tabla 14*. Personal asignado a la implementación*

Nº.	Nombre	Descripción
1	Neyser Torres Leiva	Especialista I en redes y telecomunicaciones

2	Julio Morales Chapman	Especialista II en redes y telecomunicaciones

4.1.2.3. Presupuesto del proyecto

Tabla 15. *Presupuesto asignado*

Presupuesto de contingencia		
Presupuesto	Reserva	Total
S/. 6270,00	S/. 1500,00	S/. 7770,00

Tabla 16*. Detalle del presupuesto*

Categoría	**Recurso**	**Tipo de unidades**	**Presupuesto**
Personal	Neyser torres Leiva	Horas / mensual	S/. 1000,00
	Julio Morales Chapman	Horas / mensual	S/. 1000,00
Hardware	Servidor VPN	1 und.	S/. 3500,00
	Switch TL-SG1008	1 und.	S/. 200,00
	Gabinete 6ru	1 und.	S/. 250,00
	Accesorios	1 und.	S/. 120,00
Software	Linux Ubuntu	----------	S/. 00,00
	Open VPN	----------	S/. 00,00
Movilidad	Combustible	Ruta / semanal	S/.200,00

4.1.2.4. Cronograma de actividades

Figura 6. Cronograma de actividades

4.1.3. Fase de Diseño

4.1.3.1 Planeamiento IP

Para mejorar el ordenamiento y seguridad en la red se tomó el siguiente direccionamiento IP de Sub-Red.

Tabla 17. *Sub-Redes asignadas*

Red	Máscara	Gateway	IPs utilizables
192.168.1.0	255.255.255.128	192.168.1.1	192.168.1.2 192.168.1.126
192.168.1.128	255.255.255.128	192.168.1.129	192.168.1.130 192.168.1.253

Tabla 18. *Direccionamiento a los dispositivos conectados a la red LAN*

IP	Dispositivo	Máscara
192.168.1.130	PC Operaciones	255.255.255.128
192.168.1.131	PC Almacén	255.255.255.128
192.168.1.132	PC Diseño	255.255.255.128
192.168.1.133	PC Asistente de Ope	255.255.255.128
192.168.1.150	Servidor VPN	255.255.255.128
192.168.1.151	Servidor de archivos	255.255.255.128
192.168.1.100	Cámara exterior	255.255.255.128
192.168.1.101	Cámara Fabricación	255.255.255.128
192.168.1.102	Cámara Vigilancia	255.255.255.128
192.168.1.103	Cámara oficinas	255.255.255.128
192.168.1.120	Repetidor CCTV	255.255.255.128
192.168.1.121	Grabador CCTV	255.255.255.128

4.1.3.2. Diseño lógico propuesto

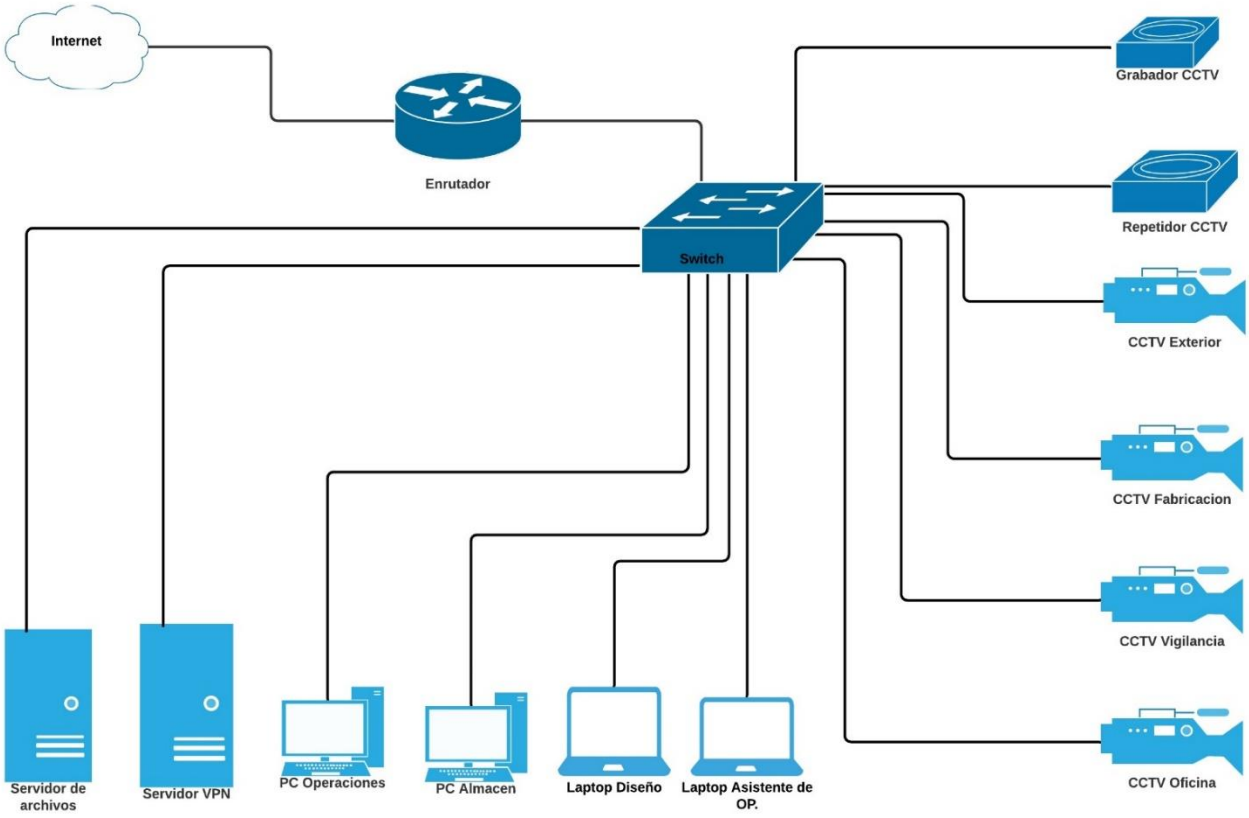


Figura 7. Topología en árbol propuesta de red

4.1.3.3. Selección de protocolos

A continuación, se nombra los dispositivos que trabajan en cada una de las capas del modelo de referencia OSI, Desde los dispositivos físicos hasta la capa de aplicación.

Tabla 19. *Protocolos y estándares nivel físico y lógico - Modelo OSI*

Nº Capa	Protocolo / Estándar	Dispositivo
1. Física	- Ethernet 100 / 1000 Base -TX - FastEthernet - GigaEthernet	Switch TL-SG108
2. Enlace de datos	- IEEE 802.1Q - IEEE 202.3	Switch TL-SG108

3. Red	- Red - OpenVPN	Modem Router Servidor VPN
4. Transporte	- TCP / IP - UDP	Servidor VPN

Tabla 20. Protocolos y estándares a nivel software - Modelo OSI

Nº Capa	Protocolo / Estándar	Dispositivo
5. Sesión	- Telnet - Linux	----------
6. Presentación	- HTTP - HTTPS	----------
7. Aplicación	- SMTP - SNMP	----------

4.1.3.4. Seguridad en la Red Privada Virtual Propuesto

OpenVPN es un producto muy seguro que puede utilizar claves de cifrado de 256 bits y códigos premium. Desde una perspectiva de seguridad, las conexiones OpenVPN son muy flexibles. SHA 256, SHA38 SHA512, RMD160 para el cifrado de autenticación utilizando un cifrado fuerte incluido como AES y Camellia. Además, puede utilizar 5 protocolos VPN: SoftEther, IKEv2 / IPSec, SSTP, L2TP / IPSec y PPTP.

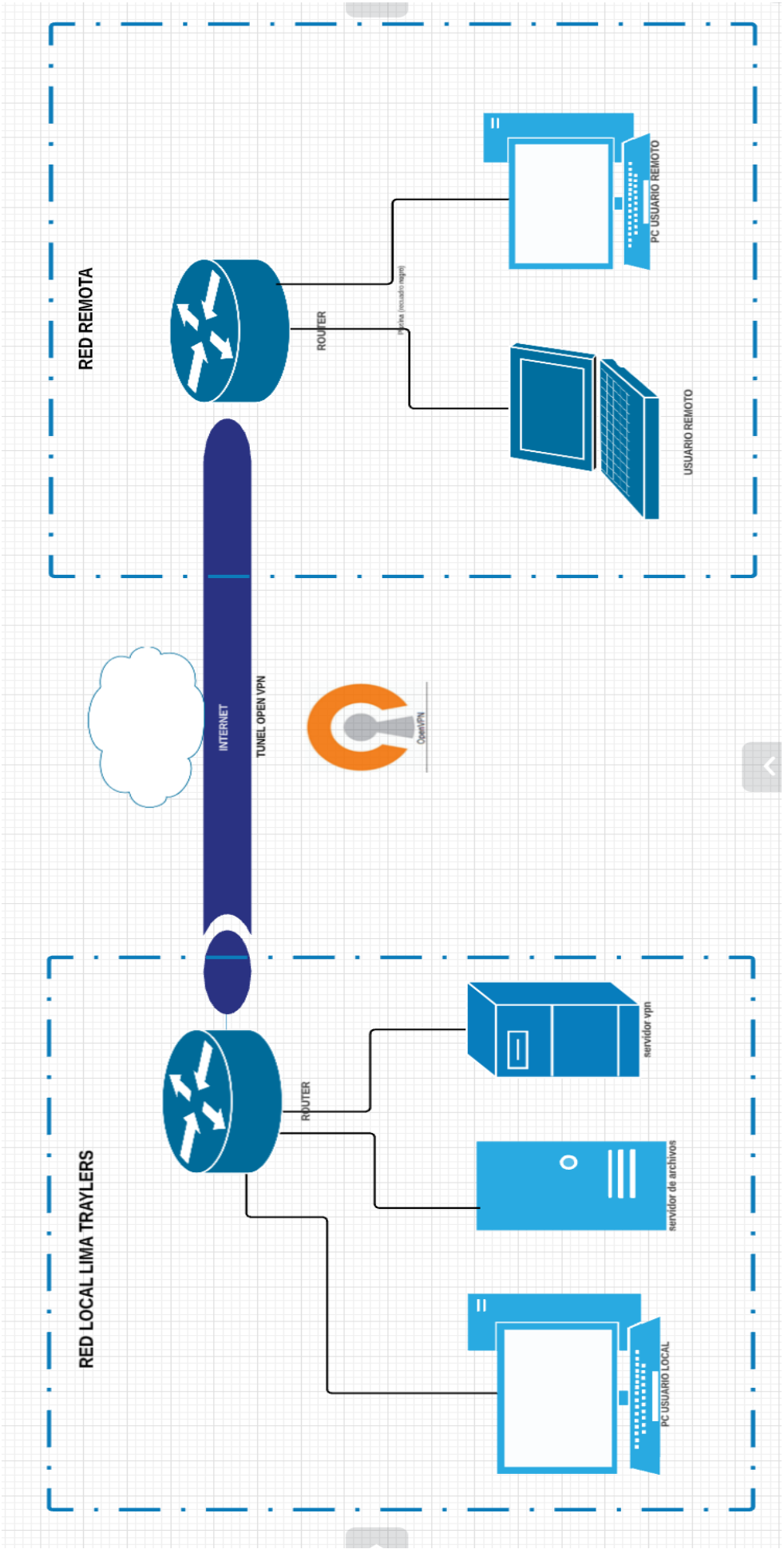


Figura 8. Topología de red VPN propuesta

4.1.3.5. Diseño físico propuesto

Servidor VPN

OpenVPN es una solución de código abierto de capa de conexión segura (SSL) que provee una diversa variedad de configuraciones. Se implementará un servidor OpenVPN bajo plataforma de software libre mediante un servidor Ubuntu Servers LTS 20.04 y luego el acceso a él desde Windows usando una máquina virtual.

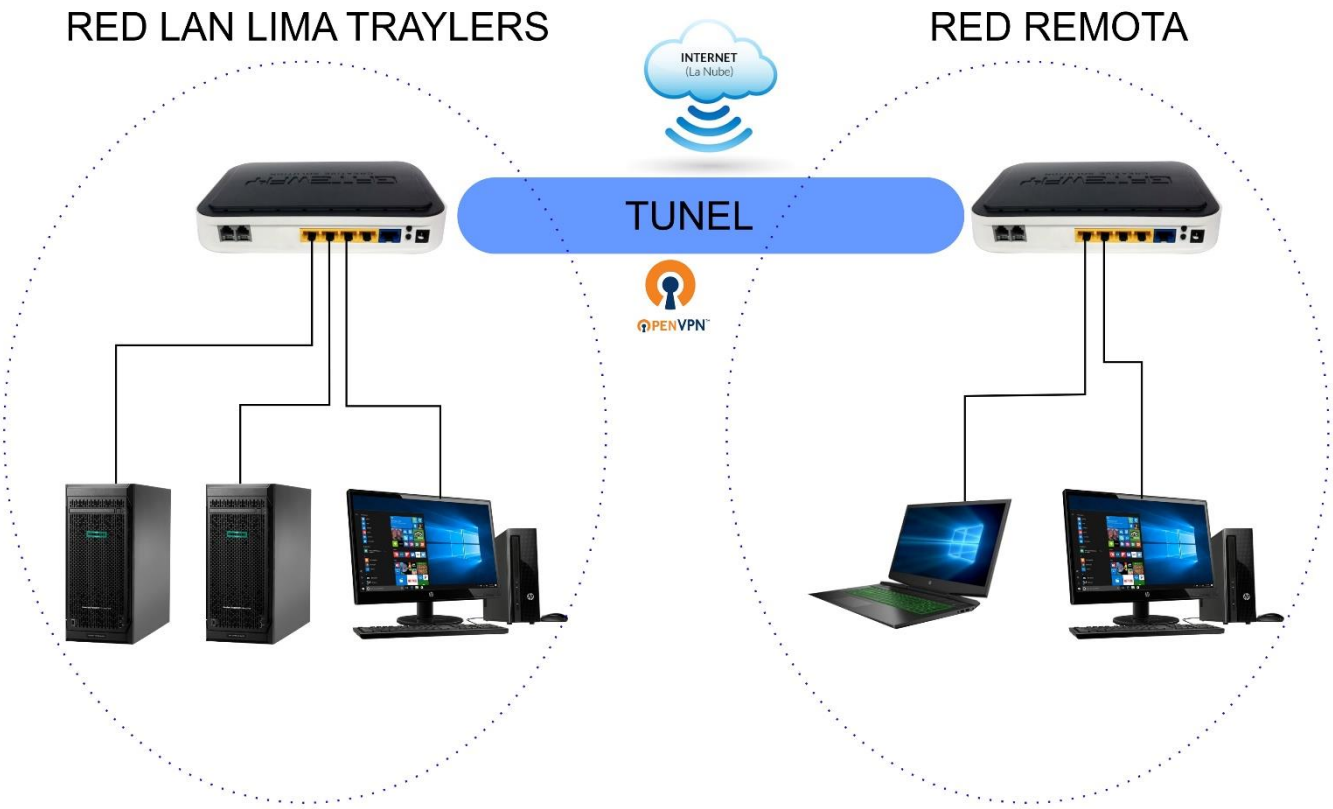


Figura 9. Diseño Físico de la red propuesta

4.1.4. Fase de Implementación

4.1.4.1 Instalación de sistema operativo

Para la implementación de la OpenVPN se instaló el sistema operativo de software libre LINUX Ubuntu Server LTS 20.04 para la estabilidad y seguridad empresarial.

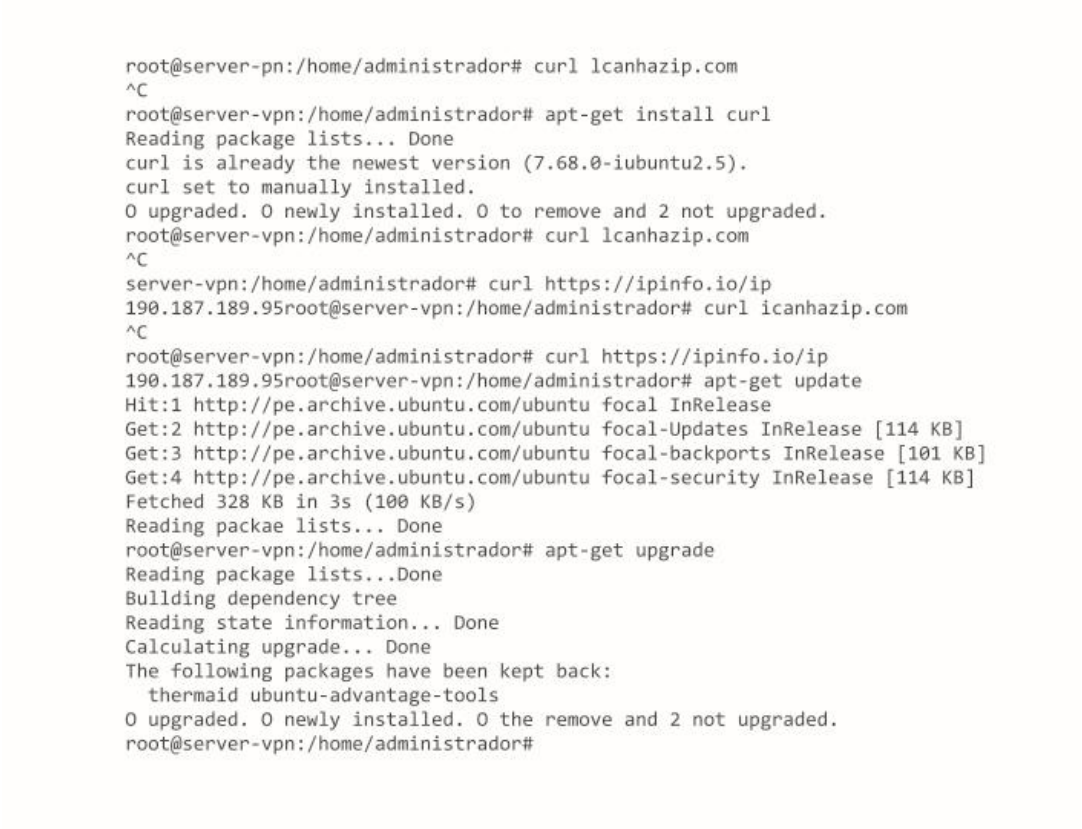


Figura 10. Instalación de sistema operativo Linux Ubuntu (Modo Consola)

Configuración de la red del sistema operativo Linux

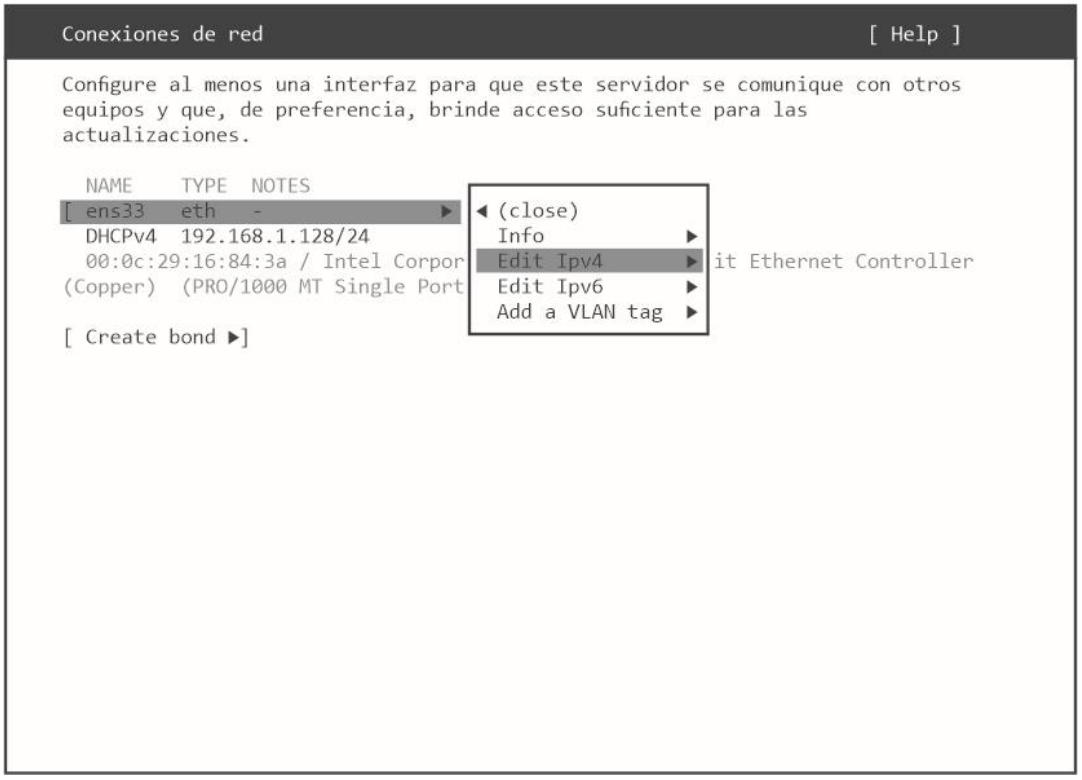


Figura 11. Configuración de red manual

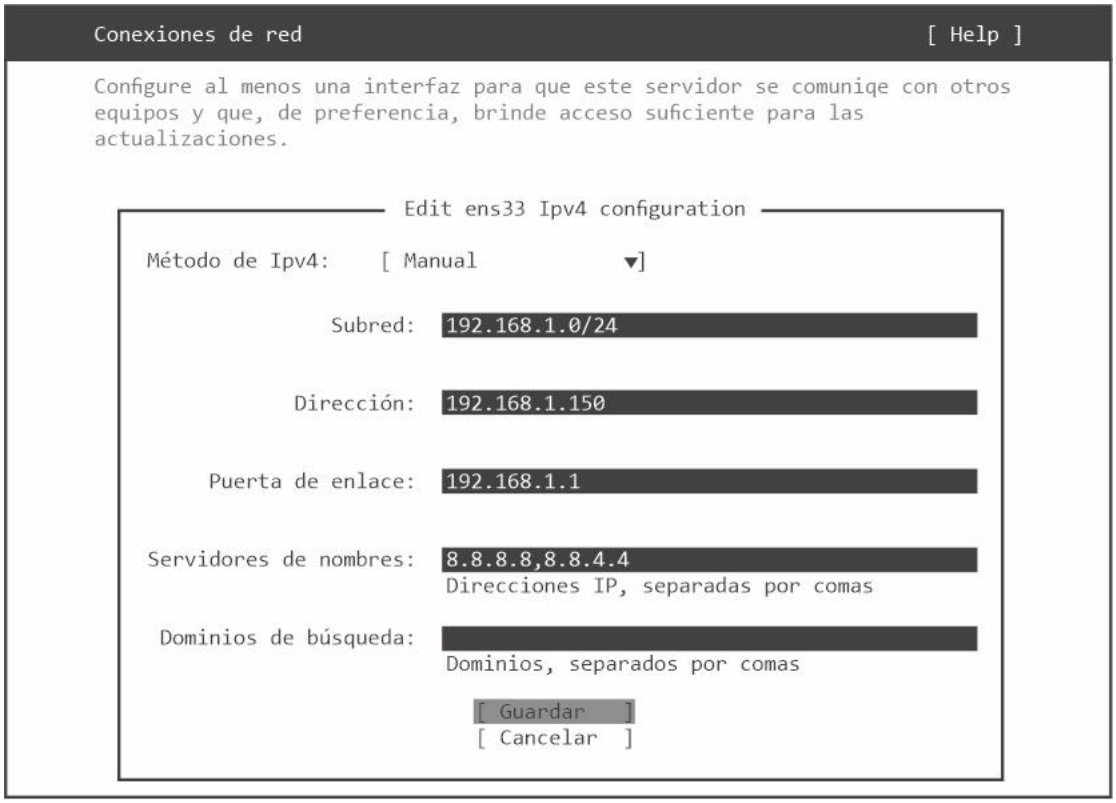


Figura 12. Configuración de red IPv4

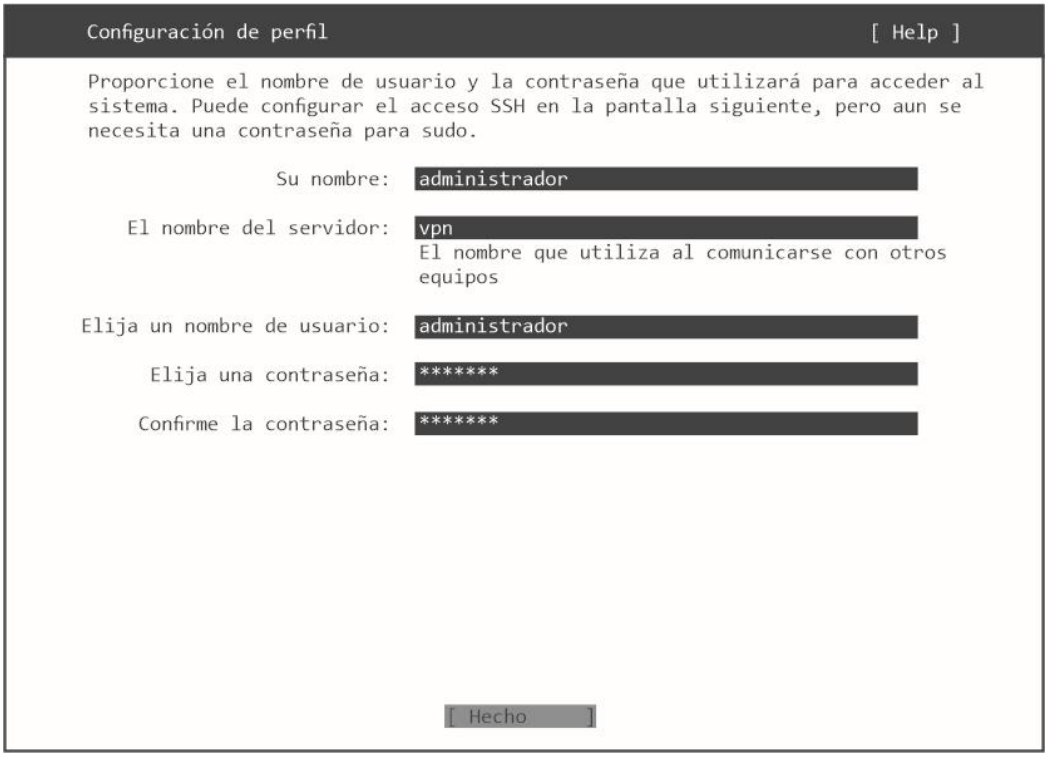


Figura 13. Configuración de perfil de usuario

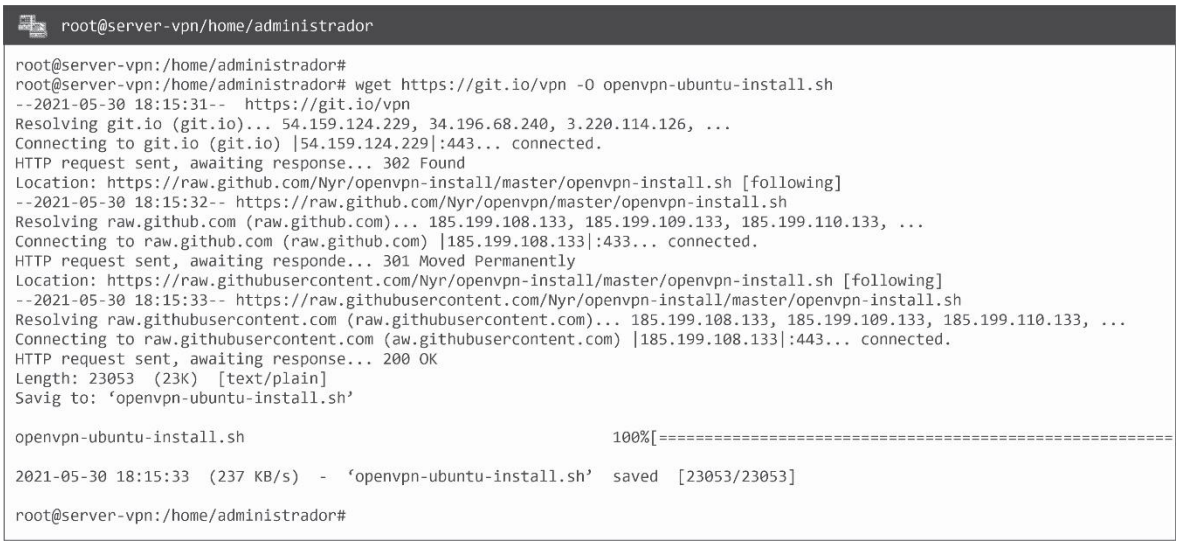


Figura 14. Descarga de OpenVPN

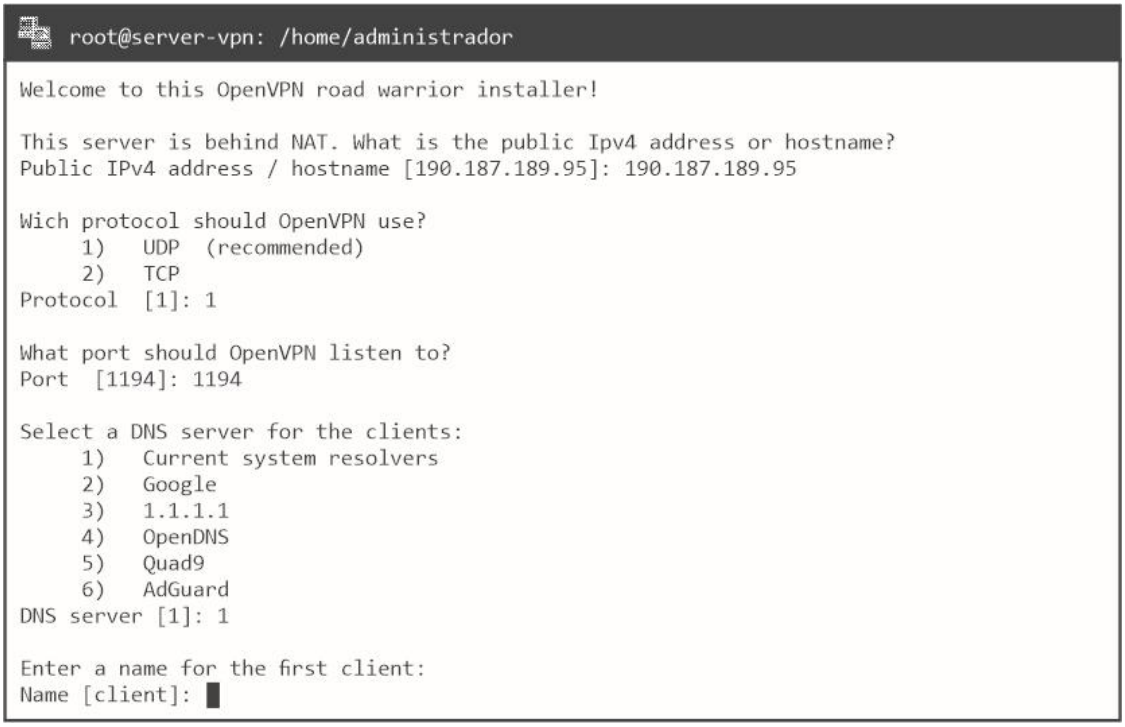


Figura 15. Instalación de OpenVPN

No.	Enable	Inter_Iface	Inter_Initial_Port	Inter_End_Port	Protocol	Intra_IP	Intra_Initial_Port	Intra_End_Port
0	Enable	DATA	8001	8001	TCP	192.168.1.45	8001	8001
1	Enable	DATA	554	554	TCP	192.168.1.45	554	554
2	Enable	DATA	2036	2036	TCP	192.168.1.45	2036	2036
3	Enable	DATA	8002	8002	TCP	192.168.1.51	8002	8002
4	Enable	DATA	553	553	TCP	192.168.1.51	553	553
5	Enable	DATA	2038	2038	TCP	192.168.1.51	2038	2038
6	Enable	190.187.189.95	1194	1194	UDP	192.168.1.150	1194	1194

Figura 16. Configuración de Puertos en el Modem Router

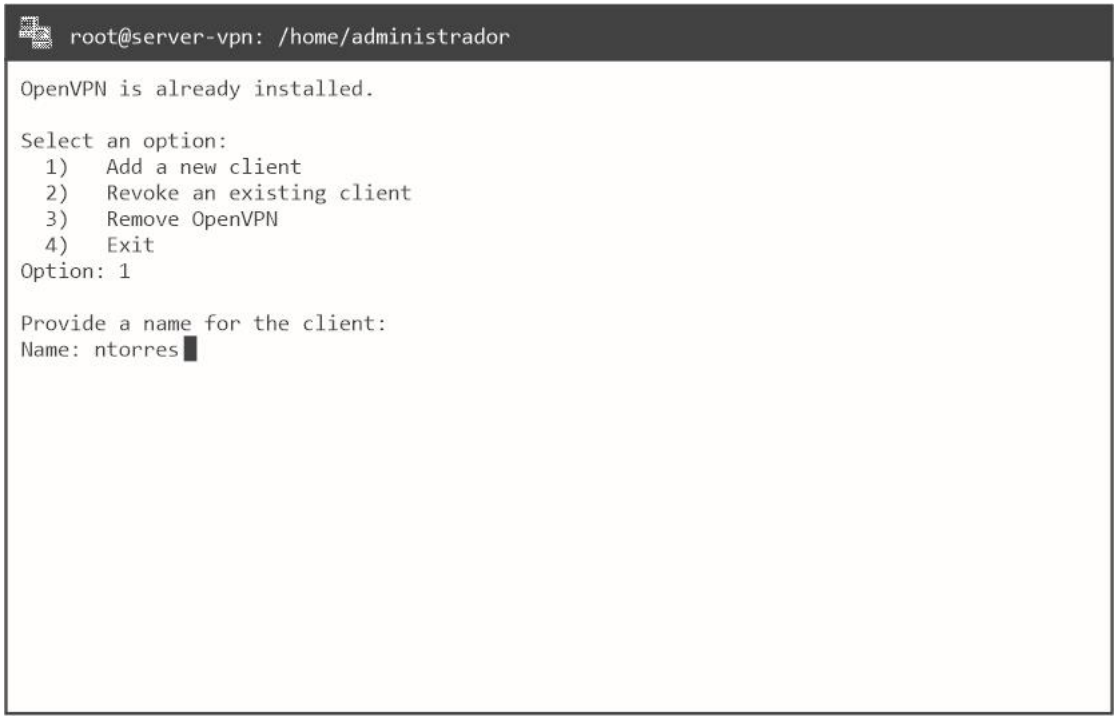


Figura 17. Creación de Usuarios OpenVPN

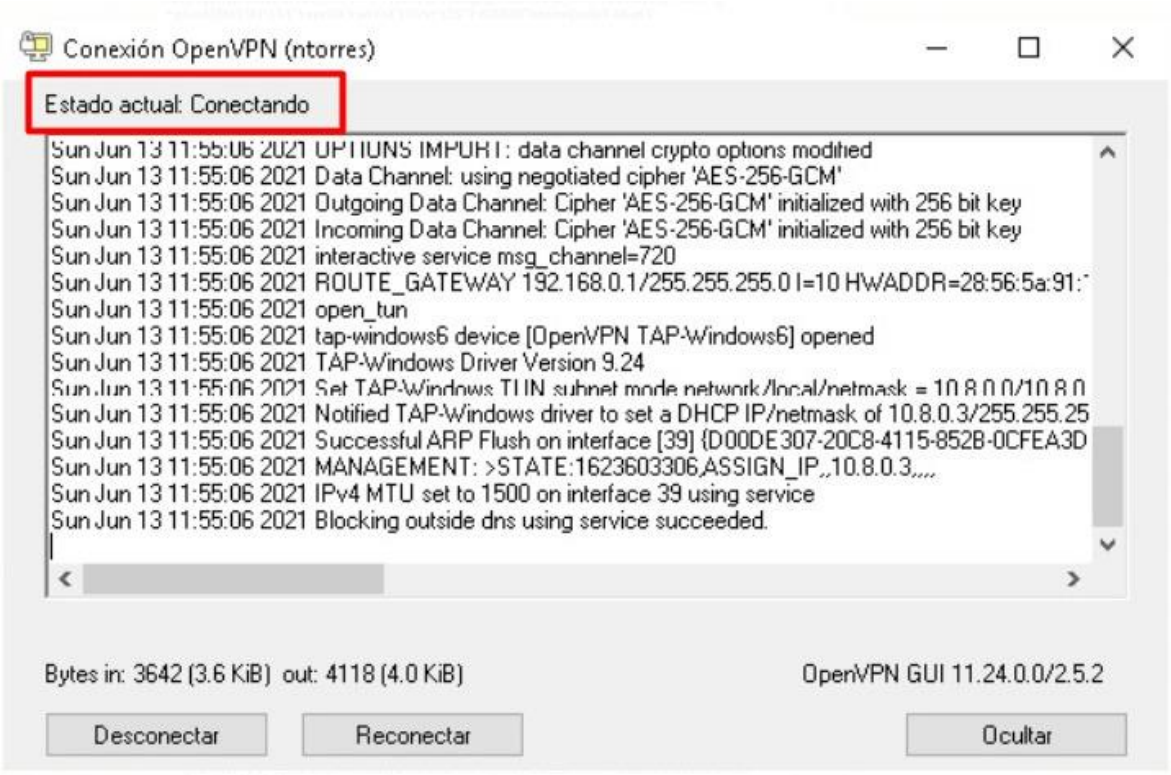


Figura 18. Configuración de OpenVPN en la PC del usuario.

Figura 19. Confirmación de conexión de OpenVPN

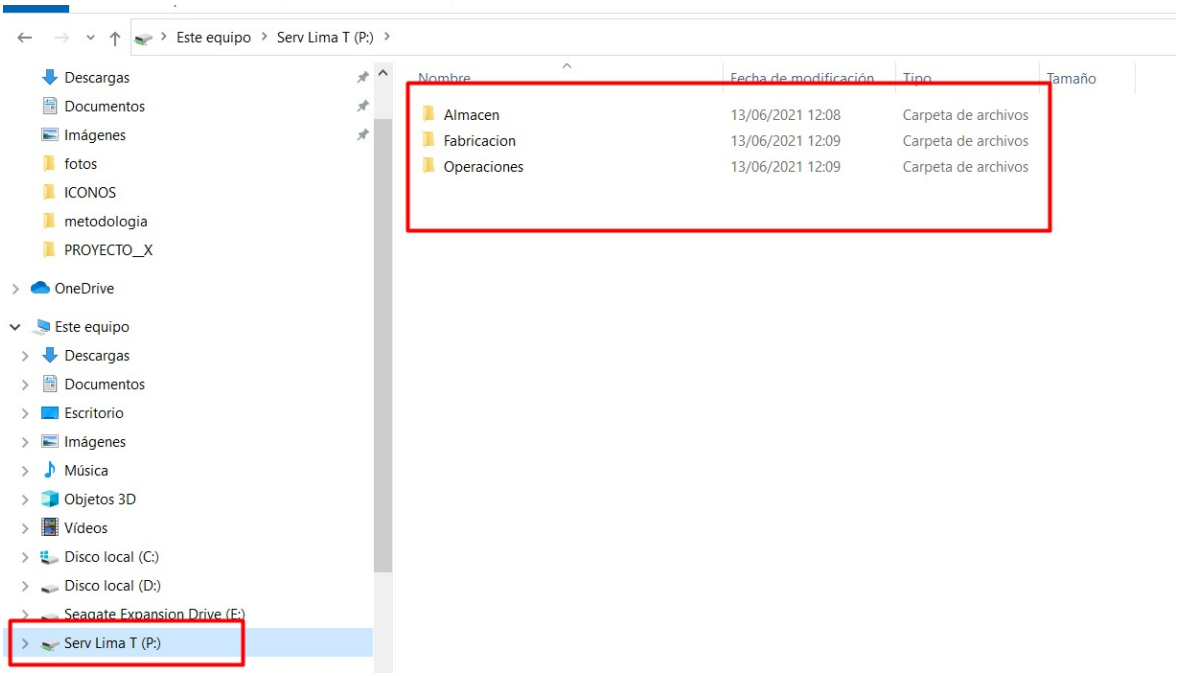


Figura 20. Usuario conectado al servidor

4.1.5. Fase de Operación

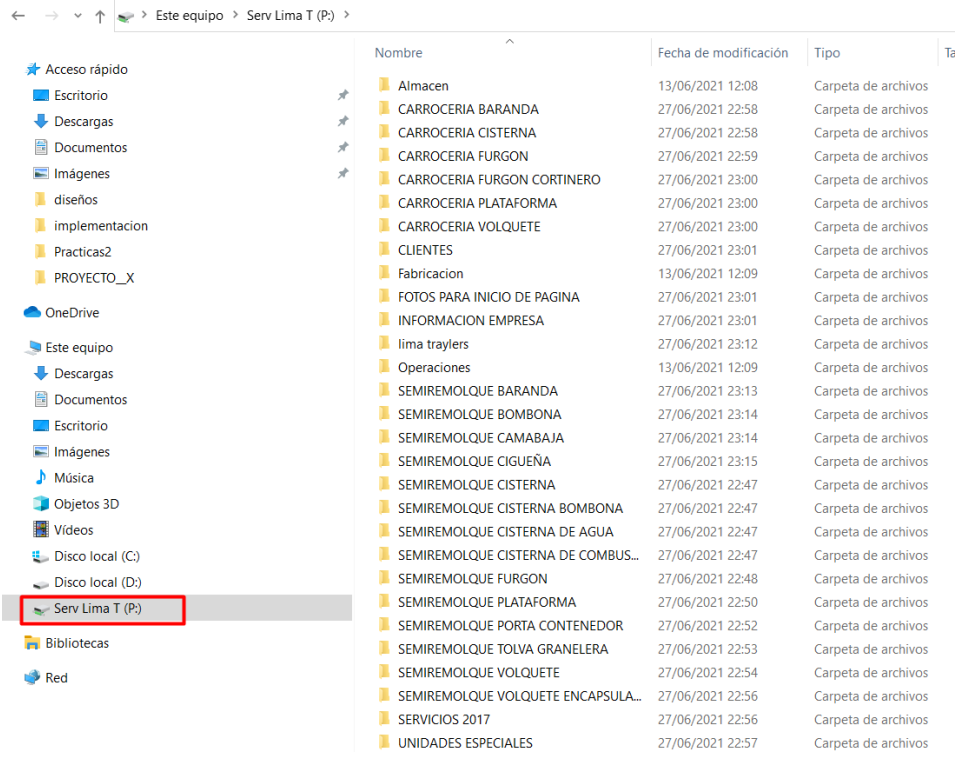


Figura 21. Acceso a carpetas compartidas a través de VPN

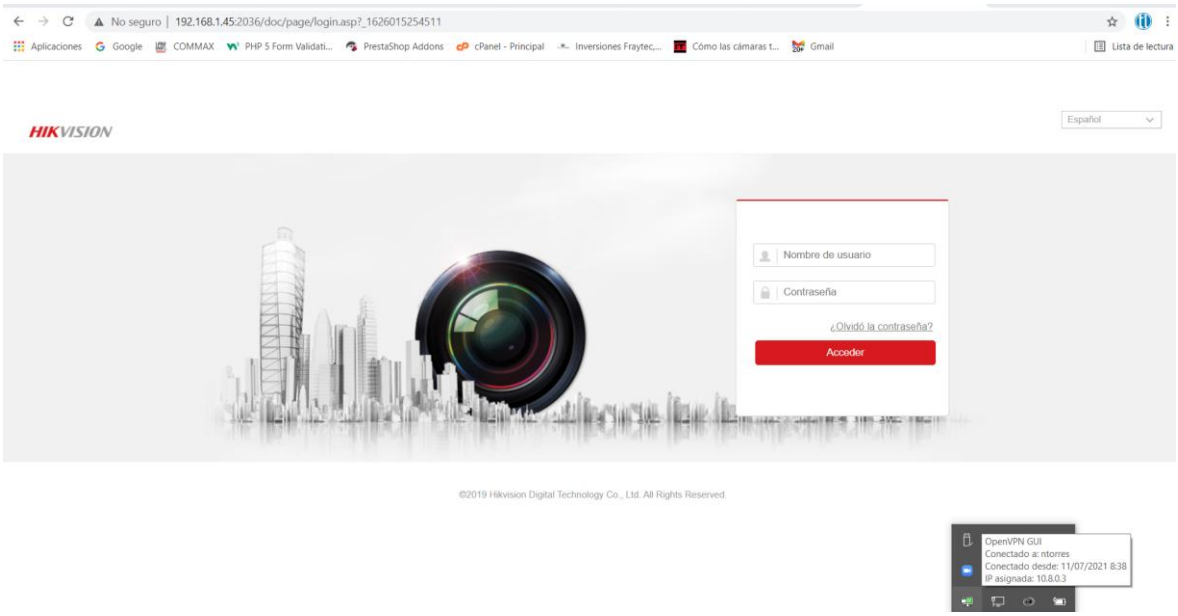


Figura 22. Acceso remoto a cámaras mediante IP local

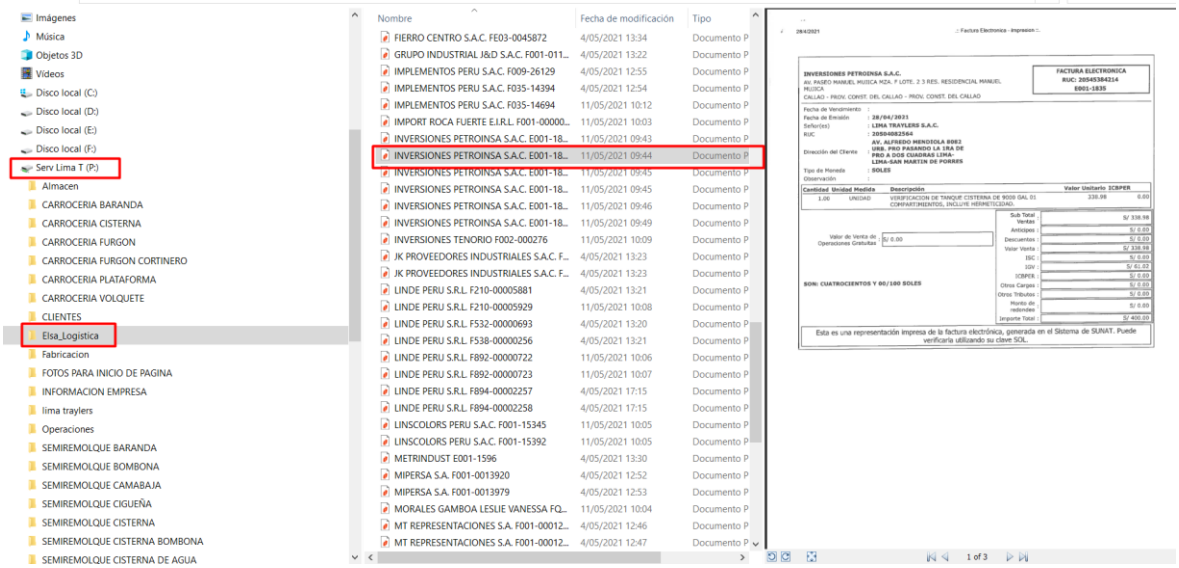


Figura 23. Usuario revisando su información de acceso remoto

4.1.6 Fase de Optimización

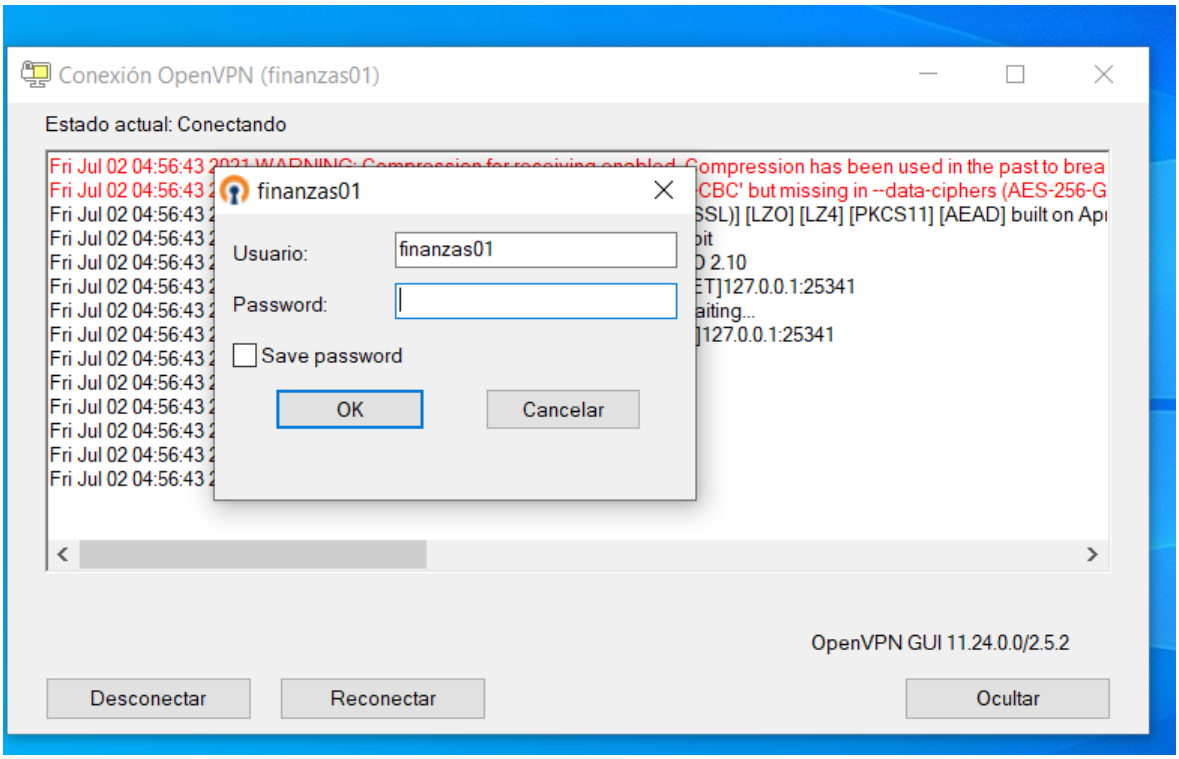


Figura 24. Conexión a la VPN por usuario y contraseña

4.2. Resultados

Tabla 21. *Resultados de PostPrueba del Gc Y PostPrueba del Ge para I1, I2, I3, I4.*

	I1: Cantidad de incidencias reportadas por los usuarios (Incidencias / Usuario)		I2: Cantidad de usuarios conectados en la red (Conexiones / Usuario)		I3: Tiempo para acceder a las carpetas compartidas (Segundos / Usuario)		I4: Nivel de Satisfacción de los usuarios (Escala de Likert)	
Nº	PostPrueba del Gc	PostPrueba del Ge	PostPrueba del Gc	PostPrueba del Ge	PostPrueba del Gc	PostPrueba del Ge	PostPrueba del Gc	PostPrueba del Ge
1	3	3	20	20	180	30	en desacuerdo	de acuerdo
2	2	1	32	22	200	40	ni acuerdo ni desacuerdo	de acuerdo
3	2	2	24	23	240	35	en desacuerdo	de acuerdo
4	1	1	26	26	280	45	ni acuerdo ni desacuerdo	totalmente de acuerdo
5	4	3	19	23	180	60	de acuerdo	totalmente de acuerdo
6	3	2	21	25	190	70	totalmente en desacuerdo	de acuerdo
7	1	0	32	20	200	40	en desacuerdo	de acuerdo
8	2	1	28	19	220	35	ni acuerdo ni desacuerdo	ni acuerdo ni desacuerdo
9	3	2	31	25	300	33	en desacuerdo	de acuerdo
10	3	0	33	22	250	45	ni acuerdo ni desacuerdo	ni acuerdo ni desacuerdo
11	6	4	23	23	280	50	de acuerdo	totalmente de acuerdo
12	4	1	25	23	220	60	totalmente en desacuerdo	ni acuerdo ni desacuerdo
13	4	4	26	25	250	50	en desacuerdo	de acuerdo
14	2	0	19	21	300	50	ni acuerdo ni desacuerdo	de acuerdo
15	3	2	15	30	290	60	ni acuerdo ni desacuerdo	ni acuerdo ni desacuerdo
16	5	4	25	22	300	30	en desacuerdo	de acuerdo
17	4	3	25	20	250	30	ni acuerdo ni desacuerdo	de acuerdo
18	3	2	26	22	240	40	totalmente en desacuerdo	totalmente de acuerdo
19	2	1	31	21	230	45	en desacuerdo	totalmente de acuerdo
20	2	2	26	25	210	50	de acuerdo	totalmente de acuerdo
21	5	5	27	23	250	65	en desacuerdo	de acuerdo
22	1	1	20	25	260	55	ni acuerdo ni desacuerdo	ni acuerdo ni desacuerdo
23	5	5	26	25	245	45	en desacuerdo	de acuerdo
24	0	0	24	23	250	38	totalmente en desacuerdo	ni acuerdo ni desacuerdo
25	3	3	31	22	270	48	de acuerdo	totalmente de acuerdo
26	4	3	27	26	260	35	en desacuerdo	de acuerdo
27	6	6	28	28	180	55	totalmente en desacuerdo	totalmente de acuerdo
28	6	3	26	24	180	65	en desacuerdo	totalmente de acuerdo
29	3	3	34	19	200	35	ni acuerdo ni desacuerdo	de acuerdo
30	4	4	20	21	220	40	totalmente en desacuerdo	ni acuerdo ni desacuerdo

4.3. Prueba de normalidad

El estudio utilizó la prueba de Anderson-Darling. Esta prueba compara la función de distribución acumulativa empírica de los datos de la muestra con la distribución acumulativa experimental de los datos de la muestra que se esperaría si los datos fueran normales.

4.3.1. I1: Cantidad de incidencias reportadas por los usuarios

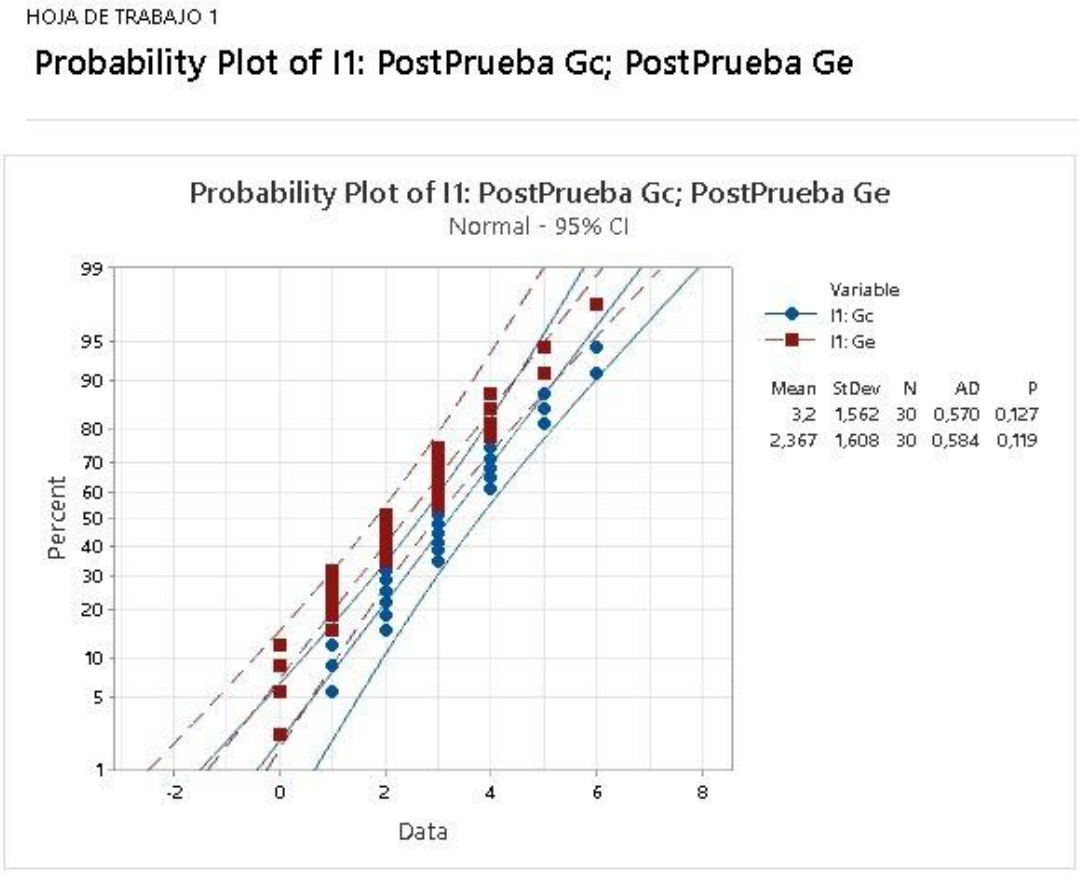


Figura 25. Prueba de normalidad para I1

Se observa que, para el indicador en la PostPrueba del Ge y la PostPrueba del Gc p (0,127 y 0,119) > α (0,05). En consecuencia, los datos del indicador presentan un comportamiento normal.

4.3.2. I2: Cantidad de usuarios conectados en la red

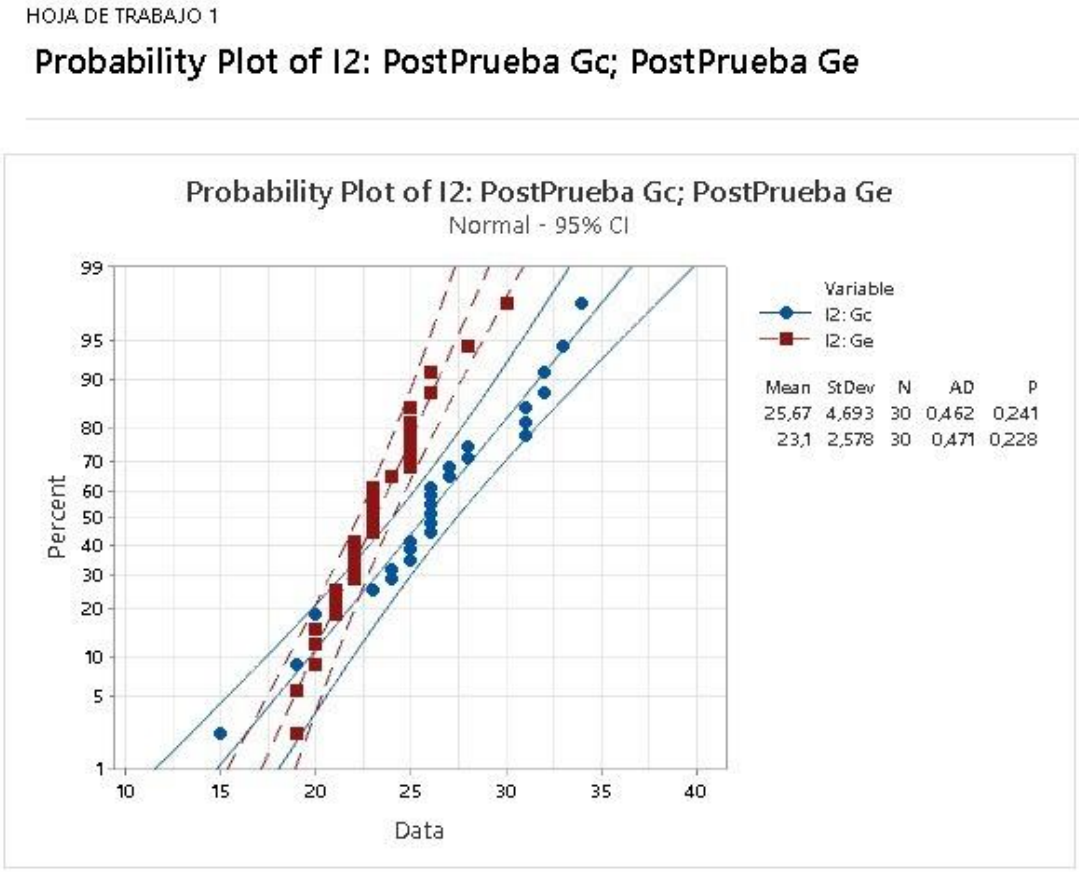


Figura 26. Prueba de normalidad para I2

Se aprecia que, para el indicador en la PostPrueba del Ge y la PostPrueba del Gc p (0.242 y 0.228) > α (0.05). Por consiguiente, los datos del indicador presentan un comportamiento normal.

4.3.3. I3: Tiempo para acceder a las carpetas compartidas

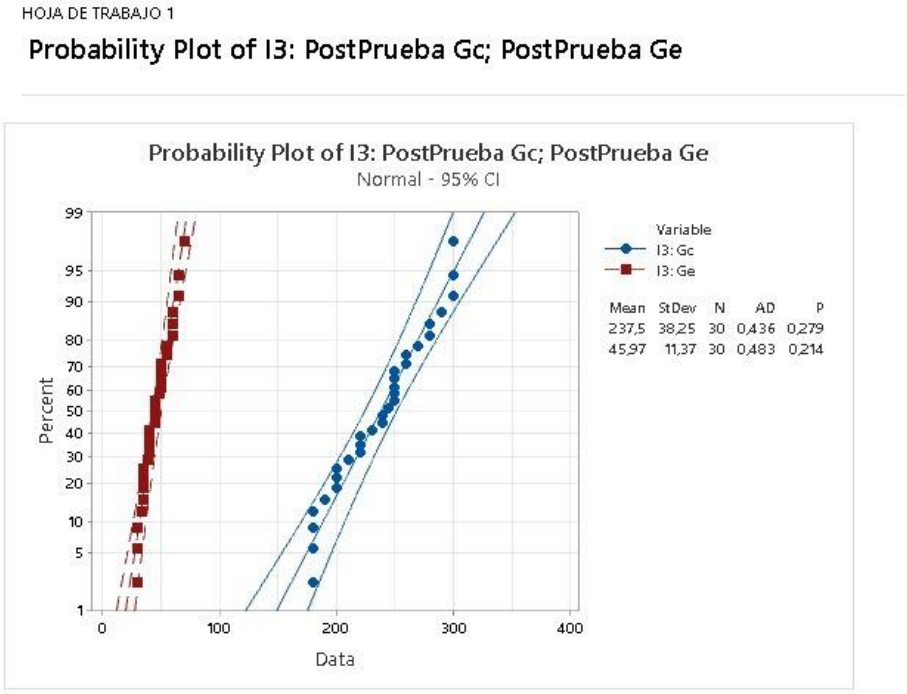


Figura 27. Prueba de normalidad para I3

Se observa que, para el indicador en la PostPrueba del Ge y la PostPrueba del Gc p (0.279 y 0.214) > α (0.05). Por tanto, los datos del indicador presentan un comportamiento normal.

4.4. Análisis de resultados

4.4.1. I1: Cantidad de incidencias reportadas por los usuarios

Tabla 22. *Resultados PostPrueba del Gc y PostPrueba del Ge para el I1*

	I1: Cantidad de incidencias reportadas por los usuarios (Incidencias / Día)			
	PostPrueba del Gc	PostPrueba del Ge		
	3	3	3	3
	2	1	1	1
	2	2	2	2
	1	1	1	1
	4	3	3	3
	3	2	2	2
	1	0	0	0
	2	1	1	1
	3	2	2	2
	3	0	0	0
	6	4	4	4
	4	1	1	1
	4	4	4	4
	2	0	0	0
	3	2	2	2
	5	4	4	4
	4	3	3	3
	3	2	2	2
	2	1	1	1
	2	2	2	2
	5	5	5	5
	1	1	1	1
	5	5	5	5
	0	0	0	0
	3	3	3	3
	4	3	3	3
	6	6	6	6
	6	3	3	3
	3	3	3	3
	4	4	4	4
Promedio	**3,20**	**2,37**		
Meta Planteada			**1**	
Nº menor a Promedio		16	10	23
% menor a Promedio		**53,3**	**33,3**	**76,7**

El 53.3 % de la Cantidad de incidencias reportadas por los usuarios (Incidencias / Día) en la PostPrueba del Ge fueron menores que su Cantidad promedio. El 33.3 % de la Cantidad de incidencias reportadas por los usuarios en la PostPrueba del Ge fueron menores que su Meta planteada. El 76.7 % de la Cantidad de incidencias reportadas por los usuarios en la PostPrueba del Ge fueron menores que la Cantidad promedio en la PostPrueba del Gc.

4.4.2. I2: Cantidad de usuarios conectados en la red

Tabla 23. *Resultados de PostPrueba del Gc y PostPrueba de Ge para I2*

I2: Cantidad de usuarios conectados en la red (Conexiones / Día)			
PostPrueba del Gc	PostPrueba del Ge		
20	20	20	20
32	22	22	22
24	23	23	23
26	26	26	26
19	23	23	23
21	25	25	25
32	20	20	20
28	19	19	19
31	25	25	25
33	22	22	22
23	23	23	23
25	23	23	23
26	25	25	25
19	21	21	21
15	30	30	30
25	22	22	22
25	20	20	20
26	22	22	22
31	21	21	21
26	25	25	25
27	23	23	23
20	25	25	25
26	25	25	25
24	23	23	23
31	22	22	22

	27	26	26	26
	28	28	28	28
	26	24	24	24
	34	19	19	19
	20	21	21	21
Promedio	**25,67**	**23,10**		
Meta Planteada			**22**	
Nº menor a Promedio		19	13	26
% menor a Promedio		**63,3**	**43,3**	**86,7**

El 63.3 % de la Cantidad de usuarios conectados en la red (Conexiones / Día) reportadas por los usuarios en la PostPrueba del Ge fueron menores que su Cantidad promedio. El 43.3 % de la Cantidad de usuarios conectados en la red en la PostPrueba del Ge fueron menores que su Meta planteada. El 86.7 % de la Cantidad de usuarios conectados en la red en la PostPrueba del Ge fueron menores que la Cantidad promedio en la PostPrueba del Gc.

4.4.3. I3: Tiempo para acceder a las carpetas compartidas

Tabla 24. *Resultados de PostPrueba del Gc y PostPrueba del Ge para el I3.*

	I3: Tiempo para acceder a las carpetas compartidas (Segundos / Usuario)			
	PostPrueba del Gc	PostPrueba del Ge		
	180	30	30	30
	200	40	40	40
	240	35	35	35
	280	45	45	45
	180	60	60	60
	190	70	70	70
	200	40	40	40
	220	35	35	35
	300	33	33	33
	250	45	45	45
	280	50	50	50
	220	60	60	60
	250	50	50	50
	300	50	50	50
	290	60	60	60
	300	30	30	30
	250	30	30	30
	240	40	40	40
	230	45	45	45
	210	50	50	50
	250	65	65	65
	260	55	55	55
	245	45	45	45
	250	38	38	38
	270	48	48	48
	260	35	35	35
	180	55	55	55
	180	65	65	65
	200	35	35	35
	220	40	40	40
Promedio	**237,50**	**45,97**		
Meta Planteada			**50**	
Nº menor a Promedio		17	22	30
% menor a Promedio		**56,7**	**73,3**	**100,0**

El 56.7 % de los Tiempos para acceder a las carpetas compartidas (Segundos / Usuario) en la PostPrueba del Ge fueron menores que su Tiempo promedio. El 73.3 % de los Tiempos para acceder a las carpetas compartidas en la PostPrueba del Ge fueron menores que su Meta planteada. El 100.0 % de los Tiempos para acceder a las carpetas compartidas en la PostPrueba del Ge fueron menores que el Tiempo promedio en la PostPrueba del Gc.

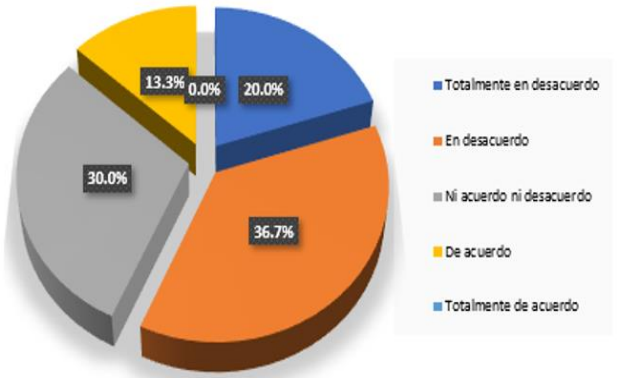
I4: Nivel de satisfacción del usuario en la red

Tabla 25. *Valores de PostPrueba Gc*

Nro. Medición	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Valor	EnDe	NAcNDe	EnDe	NAcNDe	DeAc	ToEnDe	EnDe	NAcNDe	EnDe	NAcNDe	DeAc	ToEnDe	EnDe	NAcNDe	NAcNDe
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	EnDe	NAcNDe	ToEnDe	EnDe	DeAc	EnDe	NAcNDe	EnDe	ToEnDe	DeAc	EnDe	ToEnDe	EnDe	NAcNDe	ToEnDe

Estado	Frecuencia	%
Totalmente en desacuerdo	6	20.0
En desacuerdo	11	36.7
Ni acuerdo ni desacuerdo	9	30.0
De acuerdo	4	13.3
Totalmente de acuerdo	0	0.0
TOTAL	30	100

Estado	Frecuencia	%
Buenos	4	13.3
Malos	26	86.7



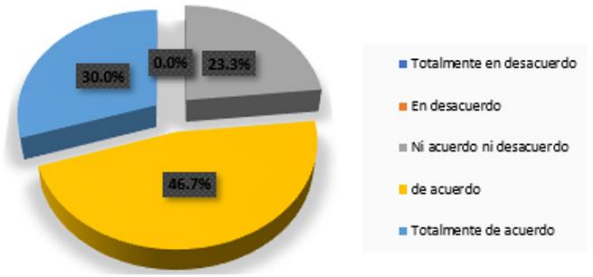
El 20.0 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como Totalmente en Desacuerdo por los usuarios. El 36.7 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como En Desacuerdo por los usuarios. El 30.0 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como Ni Acuerdo Ni Desacuerdo por los usuarios. Sólo el 13.3 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como De Acuerdo por los usuarios. Se precisa que el 13.3 % de las ocasiones el Nivel de Satisfacción de los Usuarios es Buena. Se precisa que el 86.7 % de las ocasiones el Nivel de Satisfacción de los Usuarios es Mala.

Tabla 26.*Valores de la PostPrueba Ge*

Nro. Medición	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Valor	DeAc	DeAc	DeAc	ToDeAc	ToDeAc	DeAc	DeAc	NAcNDe	DeAc	NAcNDe	ToDeAc	NAcNDe	DeAc	DeAc	NAcNDe
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	DeAc	DeAc	ToDeAc	ToDeAc	ToDeAc	DeAc	NAcNDe	DeAc	NAcNDe	ToDeAc	DeAc	ToDeAc	ToDeAc	DeAc	NAcNDe

Estado	Frecuencia	%
Totalmente en desacuerdo	0	0.0
En desacuerdo	0	0.0
Ni acuerdo ni desacuerdo	7	23.3
de acuerdo	14	46.7
Totalmente de acuerdo	9	30.0
TOTAL	30	100

Estado	Frecuencia	%
Buenos	23	76.7
Malos	7	23.3



Sólo el 23.3 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como Ni Acuerdo Ni Desacuerdo por los usuarios. El 46.7 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como De Acuerdo por los usuarios. El 30.0 % de las ocasiones el Nivel de Satisfacción de los Usuarios fue registrado como Totalmente de Acuerdo por los usuarios. Se precisa que sólo el 76.7 % de las ocasiones el Nivel de Satisfacción de los Usuarios es Buena. Se precisa que el 23.3 % de las ocasiones el Nivel de Satisfacción de los Usuarios es Mala.

4.5. Contrastación de la hipótesis

Contrastación para H1 (Cantidad de incidencias reportadas por los usuarios).

H1: Si usa una VPN basada en metodología PPDIOO disminuye la cantidad de incidencias reportadas por los usuarios.

Hi: El uso de una VPN basada en metodología PPDIOO disminuye la cantidad de incidencia reportadas por los usuarios (PostPrueba del Ge) en relacion a la muestra a la que ni se aplicó (PostPrueba del Gc).

Se llevó a cabo una medición sin el uso de una VPN (PostPrueba de Gc) y otra con el uso de la VPN (PostPrueba Ge)

Tabla 27. *Valores de la PostPrueba Gc y Ge*

PostPrueba Gc	3	2	2	1	4	3	1	2	3	3	6	4	4	2	3
	5	4	3	2	2	5	1	5	0	3	4	6	6	3	4

PostPrueba Ge	3	1	2	1	3	2	0	1	2	0	4	1	4	0	2
	4	3	2	1	2	5	1	5	0	3	3	6	3	3	4

Planteamiento de las hipótesis nula y alterna

H0: El uso de una VPN incrementa la **cantidad de incidencia reportadas por los usuarios** (PostPrueba del Ge) en relación a la muestra a la que no se aplicó (PostPrueba del Gc).

Ha: El uso de una VPN disminuye la **cantidad de incidencias reportadas por los usuarios** (PostPrueba del Ge) en relación a la muestra a la que no se aplicó (PostPrueba del Gc).

μ1= Media poblacional de la cantidad de incidencias reportadas por los usuarios en la PostPrueba de Gc.

μ2= Media poblacional de la cantidad de incidencias reportadas por los usuarios en la PostPrueba de Gc.

Ho: $\mu 1 \leq \mu 2$

Ha: $\mu 1 > \mu 2$

Estadístico de prueba t de Student para el I1

Prueba T e IC de dos muestras: I1: Gc; I1: Ge

Método

μ_1: media de población de I1: Gc
μ_2: media de población de I1: Ge
Diferencia: $\mu_1 - \mu_2$

No se presupuso igualdad de varianzas para este análisis.

Estadísticas descriptivas

Muestra	N	Media	Desv.Est.	Error estándar de la media
I1: Gc	30	3,20	1,56	0,29
I1: Ge	30	2,37	1,61	0,29

Estimación de la diferencia

Diferencia	IC de 95% para la diferencia
0,833	(0,014; 1,653)

Prueba

Hipótesis nula H_0: $\mu_1 - \mu_2 = 0$
Hipótesis alterna H_1: $\mu_1 - \mu_2 \neq 0$

Valor T	GL	Valor p
2,04	57	0,046

Figura 28. Prueba de t de Student para el I1

Decisión Estadística

Por lo tanto, el valor de p = 0,046 < α (0,05), por lo cual significa que los resultados proporcionan la evidencia precisa para rechazar la hipótesis nula (H_0), por ello la hipótesis alterna (Ha) es aceptada, se concluye que la prueba es significativa.

Contrastación para H2 (Cantidad de usuarios conectados a la red)

H1: Si usa una VPN basada en metodología PPDIOO gestiona la cantidad de usuarios conectados a la red.

Hi: El uso de una VPN basada en metodología PPDIOO gestiona la cantidad de usuarios conectados a la red (PostPrueba de Ge) con respecto a la muestra a la que no se aplicó (PostPrueba Gc).

Se realizó una Medición con el uso de una VPN (PostPrueba del Ge) y otra sin el uso de la VPN (PostPrueba Gc).

Tabla 28. *Valores de la PostPrueba Gc y Ge para I2*

PostPrueba Gc	20	32	24	26	19	21	32	28	31	33	23	25	26	19	15
	25	25	26	31	26	27	20	26	24	31	27	28	26	34	20

PostPrueba Ge	20	22	23	26	23	25	20	19	25	22	23	23	25	21	30
	22	20	22	21	25	23	25	25	23	22	26	28	24	19	21

Planteamiento de las Hipótesis nula y alterna

H0: El uso de una VPN no gestiona la cantidad de usuarios conectados a la red (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

Ha: El uso de una VPN gestiona la cantidad de usuarios conectados a la red (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

μ1= Media poblacional de la exactitud de la respuesta en la PostPrueba del Gc.

μ2= Media Poblacional de la exactitud de la respuesta en la PosPrueba del Ge.

H0: $\mu 1 \geq \mu 2$

Ha: $\mu 1 < \mu 1$

Estadísticos de Prueba t de Student para el I2

HOJA DE TRABAJO 1

Two-Sample T-Test and CI: PostPrueba Gc; PostPrueba Ge

Method

μ_1: population mean of I2: Gc
μ_2: population mean of I2: Ge
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
I2: Gc	30	25,67	4,69	0,86
I2: Ge	30	23,10	2,58	0,47

Estimation for Difference

Difference	95% CI for Difference
2,567	(0,598; 4,536)

Test

Null hypothesis H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis H_1: $\mu_1 - \mu_2 \neq 0$

T-Value	DF	P-Value
2,63	45	0,012

Figura 29. Prueba de t de Student para el I2

Decisión Estadística

Por lo tanto, el valor de p = 0,012 < α (0,05), por lo cual significa que los resultados proporcionan la evidencia precisa para rechazar la hipótesis nula (H_0), por ello la hipótesis alterna (Ha) es aceptada, se concluye que la prueba es significativa.

Contrastación para la H3 (Tiempo para acceder a las carpetas compartidas).

H1: Si usa una VPN basada en metodología PPDIOO disminuye el tiempo para acceder a las carpetas compartidas

Hi: El uso de una VPN basada en metodología PPDIOO disminuye el tiempo para acceder a las carpetas compartidas (PostPrueba de Ge) con respecto a la muestra a la que no se aplicó (PostPrueba Gc).

Se realizó una medición con el uso de una VPN (PostPrueba del Ge) y otra sin el uso de la VPN (PostPrueba Gc).

Tabla 29.*Valores de la PostPrueba Gc y Ge para I3*

PostPrueba Gc	180	200	240	280	180	190	200	220	300	250	280	220	250	300	290
	300	250	240	230	210	250	260	245	250	270	260	180	180	200	220

PostPrueba Ge	30	40	35	45	60	70	40	35	33	45	50	60	50	50	60
	30	30	40	45	50	65	55	45	38	48	35	55	65	35	40

Planteamiento de las Hipótesis nula y alterna

H0: El uso de una VPN incrementa el tiempo para acceder a las carpetas compartidas (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

Ha: El uso de una VPN disminuye el tiempo para acceder a las carpetas compartidas (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

μ1= Media poblacional de la exactitud de la respuesta en la PostPrueba del Gc.

μ2= Media Poblacional de la exactitud de la respuesta en la PosPrueba del Ge.

H0: $\mu 1 \geq \mu 2$

Ha: $\mu 1 < \mu 1$

Estadísticos de Prueba t de Student para el I3

Two-Sample T-Test and CI: PostPrueba Gc; PostPrueba Ge

Method

μ_1: population mean of I3: Gc
μ_2: population mean of I3: Ge
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
I3: Gc	30	237,5	38,3	7,0
I3: Ge	30	46,0	11,4	2,1

Estimation for Difference

Difference	95% CI for Difference
191,53	(176,73; 206,34)

Test

Null hypothesis H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis H_1: $\mu_1 - \mu_2 \neq 0$

T-Value	DF	P-Value
26,29	34	0,000

Figura 30. Prueba de t de Student para el I3

Decisión Estadística

Dado que, el valor de p = 0,000 < α (0,05), por lo cual significa que los resultados proporcionan la evidencia precisa para rechazar la hipótesis nula (H_0), por ello la hipótesis alterna (Ha) es aceptada, se concluye que la prueba es significativa.

Contrastación para la H4 (Nivel de satisfacción de los usuarios en la red).

H1: Si usa una VPN basada en metodología PPDIOO incrementa el nivel de satisfacción de los usuarios

Hi: El uso de una VPN basada en metodología PPDIOO incrementa el nivel de satisfacción de los usuarios (PostPrueba de Ge) con respecto a la muestra a la que no se aplicó (PostPrueba Gc).

Se realizó una Medición con el uso de una VPN (PostPrueba del Ge) y otra sin el uso de la VPN (PostPrueba Gc).

Tabla 30. *Valores de la PostPrueba Gc y Ge para I4*

PostPrueba Gc	2	3	2	3	4	1	2	3	2	3	4	1	2	3	3
	2	3	1	2	4	2	3	2	1	4	2	5	2	3	1

PostPrueba Ge	4	4	4	5	5	4	4	3	4	3	5	3	4	4	3
	4	4	5	5	5	4	3	4	3	5	4	5	5	4	3

Planteamiento de las Hipótesis nula y alterna

H0: El uso de una VPN disminuye el nivel de satisfacción de los usuarios (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

Ha: El uso de una VPN incrementa el nivel de satisfaccion del usuario (PostPrueba del Ge) con respecto a la muestra a la que no aplicó (PostPrueba del Gc).

μ1= Media poblacional de la exactitud de la respuesta en la PostPrueba del Gc.

μ2= Media Poblacional de la exactitud de la respuesta en la PosPrueba del Ge.

H0: $\mu 1 \geq \mu 2$

Ha: $\mu 1 < \mu 1$

Estadístico de Prueba de U de Mann- Whitney para el I4

HOJA DE TRABAJO 1

Mann-Whitney: I4: Gc; I4: Ge

Method

η_1: median of I4: Gc
η_2: median of I4: Ge
Difference: $\eta_1 - \eta_2$

Descriptive Statistics

Sample	N	Median
I4: Gc	30	2
I4: Ge	30	4

Estimation for Difference

Difference	CI for Difference	Achieved Confidence
-2	(-2; -1)	95,16%

Test

Null hypothesis H_0: $\eta_1 - \eta_2 = 0$
Alternative hypothesis H_1: $\eta_1 - \eta_2 \neq 0$

Method	W-Value	P-Value
Not adjusted for ties	578,00	0,000
Adjusted for ties	578,00	0,000

Figura 31. Prueba de U Mann-Whitney para el I4

Decisión Estadística

Por lo tanto, el valor de p = 0,000 < α (0,05), por lo cual significa que los resultados proporcionan la evidencia precisa para rechazar la hipótesis nula (H_0), por ello la hipótesis alterna (Ha) es aceptada, se concluye que la prueba es significativa.

V. DISCUSIÓN

Las tecnologías de información son herramientas informáticas que permiten mejorar el intercambio de información presentada en diferentes códigos.

Las TIC han reducidos significativamente el tiempo en diversos procesos mejorando la seguridad en la comunicación, una de estas tecnologías de red es la VPN que facilita el trabajo remoto en las empresas. (Espinoza Chipane, 2018)

El uso de una conexión VPN implica conectarse entre sí a través de una red que no está conectada físicamente, como un empleado actualmente ausente o una empresa con sucursales en varias ciudades que necesitan acceso a la red privada.

Desde una perspectiva de seguridad, cuando los empleados y las empresas se conectan mediante una conexión VPN, el riesgo se reduce enormemente. El acceso está protegido, las conexiones cifradas y los empleados tienen los mismos derechos de acceso que tendrían en persona. (Ramirez Varona, 2020).

Para la implementación de una VPN se utilizó la metodología PPDIOO (Preparar, Planear, Diseñar, Implementar, Operar, Optimizar) de Cisco Systems asegurando que de cumplir con todas las fases que indica esta metodología se obtendrán resultados positivos y se cumplirá el cronograma establecido. (Munar, y otros, 2020).

I1**: Cantidad de incidencias reportadas**

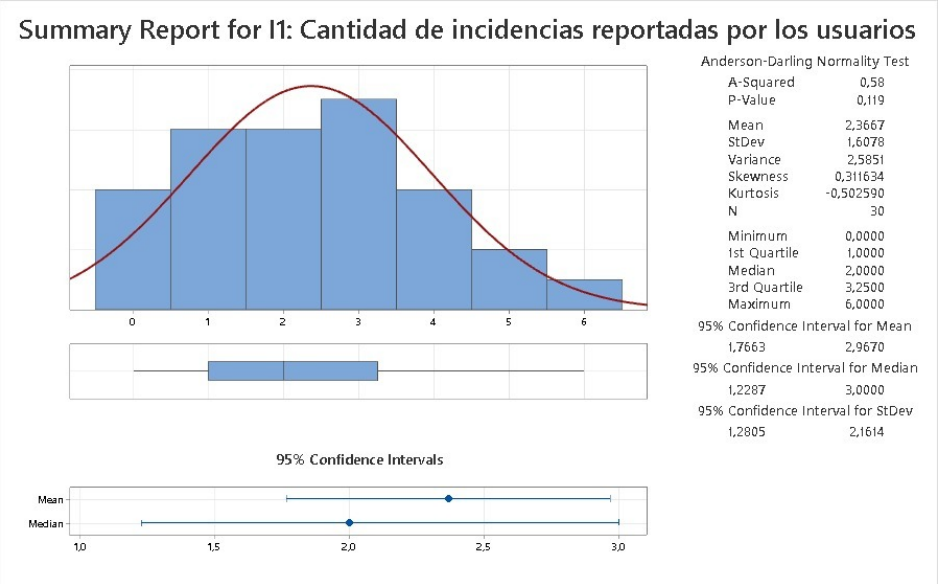


Figura 32. Resultados de estadística descriptiva para el I1

En la Figura 27, se aprecia que los datos cuentan con un comportamiento normal, ya que el valor de p (0,119) >α (0.05). Además, la distancia promedio de los valores recolectados de la cantidad de incidencias registradas por los usuarios con relación a la media es de 1.6078 incidencias con un nivel de confianza de 95% los valores de cantidad de clientes registrados por el usuario están incluidos en 2 desviaciones estándar con respecto a la media, esto significa que se encuentran entre 1.7663 y 2.9670 incidencias.

El valor obtenido de la Kurtosis es de -0.503590 indicando que existen valores de cantidad de picos muy pequeños.

Del mismo modo para el valor de asimetría el cual es de 0.311634, que señala la cantidad de incidencias reportadas son menores.

Con base a los resultados obtenidos, para el indicador de cantidad de incidencias registradas por los usuarios, se determinó que la cantidad de incidencias sin VPN es de (3 incidencias) es mayor que la cantidad de incidencias con el uso de VPN (2 incidencias) es decir que existe un decremento de 1 incidencia, equivalente a la reducción de 53.3 %; a comparación de (Espinoza Chipane, 2018), que en su investigación muestra una reducción 5 incidencias.

I2: Cantidad de usuarios conectados a la red

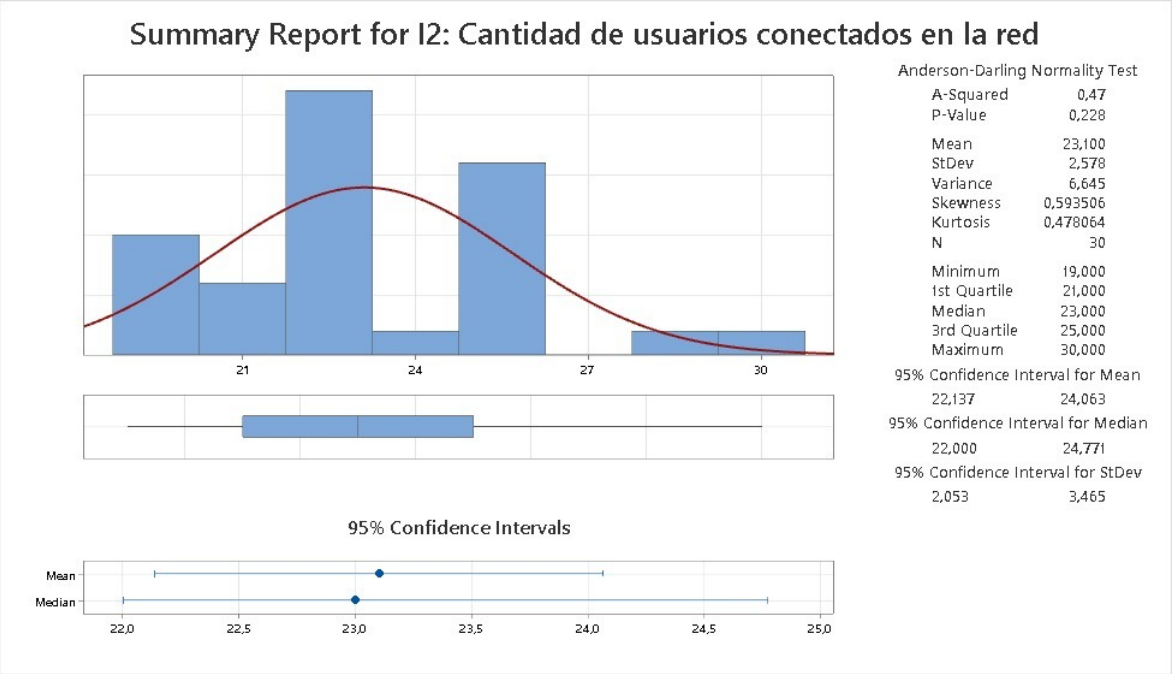


Figura 33. Resultados de estadística descriptiva para el I2

En la Figura 28, se observa que los datos tienen un comportamiento normal, ya que el valor de p (0,228) >α (0.05). Además, la distancia promedio de los valores recolectados de la cantidad de usuarios conectados a la red en relación a la media es de 2.578 usuarios conectados con un nivel de confianza de 95% los valores de cantidad de usuarios conectados a la red están incluidos en 2 desviaciones estándar con respecto a la media, esto significa que se encuentran entre 22,137 y 24,063 incidencias.

El valor obtenido de la Kurtosis es de 0.478064 indicando que existen valores de cantidad de picos muy pequeños.

Del mismo modo para el valor de asimetría el cual es de 0.593506, que señala la cantidad de usuarios conectados a la red son menores.

Con base a los resultados obtenidos, para el indicador de cantidad de usuarios conectados a la red, se determinó que la cantidad de usuarios sin VPN es de (26 usuarios) es mayor que la cantidad de usuarios con el uso de la VPN (23 usuarios) es decir que existe un decremento de 3 usuarios, equivalente a la reducción de 63.3

%; a comparación de (Ramirez Varona, 2020), que en su investigación muestra 88 usuarios conectados.

I3: Tiempo para acceder a las carpetas compartidas.

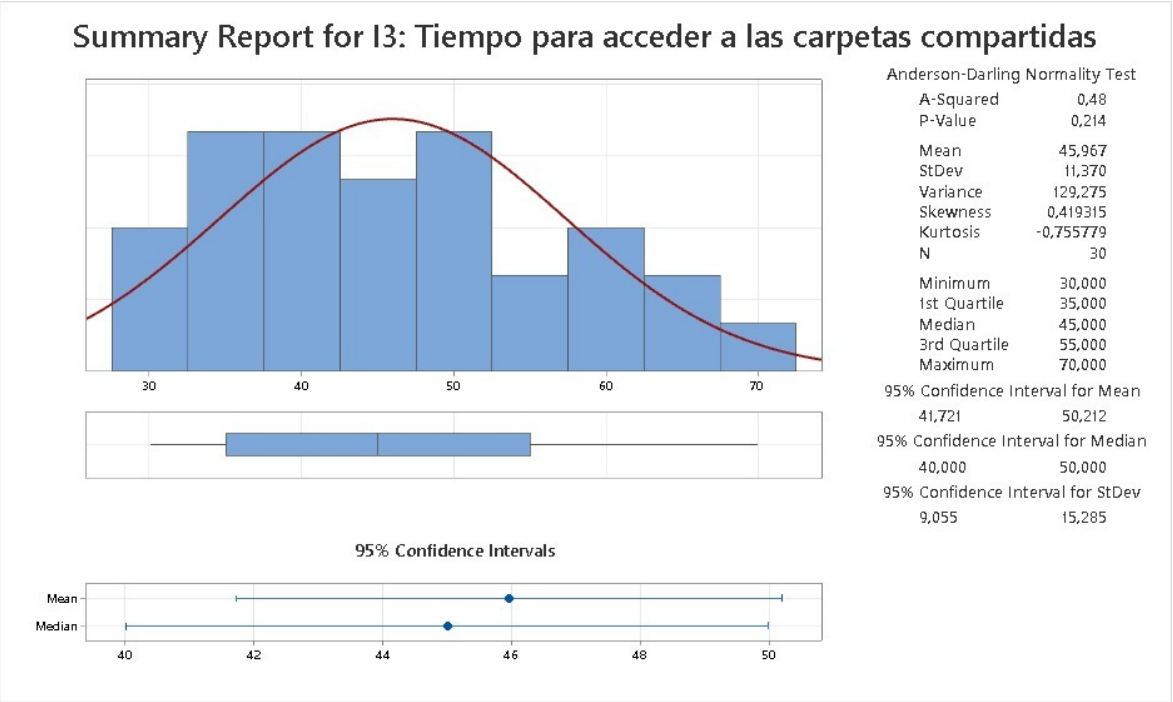


Figura 34. Resultados de estadística descriptiva para el I3

En la Figura 29, se observa que los datos tienen un comportamiento normal, ya que el valor de p (0,214) >α (0.05). Además, la distancia promedio de los valores recolectados de los tiempos de acceso a las carpetas compartidas en relación a la media es de 11,370 minutos. Con un nivel de confianza de 95% los valores de los tiempos de acceso a las carpetas compartidas están incluidos en 2 desviaciones estándar con respecto a la media, esto significa que se encuentran entre 41,721 y 50,212 Segundos.

El valor obtenido de la Kurtosis es de -0.755779 indicando que existen valores de tiempos de picos muy pequeños.

Del mismo modo para el valor de asimetría el cual es de 0.419315, que señala la mayoría de los valores de los tiempos de acceso a la as carpetas compartidas son menores.

Referente a los resultados obtenidos, para el indicador de tiempo para acceder a las carpetas compartida, se observó que antes de aplicar la VPN es de (45.97 segundos) es mayor que los tiempos con el uso de la VPN (237.50 Segundos) es decir que existe un decremento de 191 segundos, equivalente a la reducción de 56.7 %; a comparación de, (Espinoza Chipane, 2018) que en su investigación muestra una reducción de 53,3% de tiempo esto significa que existe una mejora favorable en el tiempo al ingresar a las carpetas compartidas.

I4: Nivel de satisfacción de usuario

Por último, se demostró que el nivel de satisfacción del usuario se aumentó en un 76.7 %, luego de utilizar la VPN, Garantizando que el usuario se encuentra satisfecho con la disponibilidad de la red de Lim Traylers. En cambio, en la investigación de (Sanchez, 2018), logro obtener un 90% de nivel de aprobación de los usuarios

Finalmente, los resultados confirman una mejor gestión de información ya que existe diferencias significativas entre el uso de la VPN y sin el uso de la VPN en la empresa Lima Traylers, lo que significa que hay una mejora del servicio de disponibilidad en la red.

VI. CONCLUSIONES

a) Se comprueba que, el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO, mejoró la seguridad informática en la red de Lima Traylers S.A.C.

b) Se evidencia, que el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO disminuyó la cantidad de incidencias reportadas por los usuarios.

c) Se observa, que el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO disminuyó la cantidad de usuarios conectados en la red.

d) Es notorio, que el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO disminuyó el tiempo para acceder a las carpetas compartidas.

e) Se aprecia, que el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO trajo como beneficio el aumento del nivel de satisfacción de los usuarios.

f) Se demuestra, que el uso apropiado de la metodología PPDIOO provee cuatro beneficios principales:

- Disminuye el costo total de propiedad al validar requerimientos tecnológicos y planificación para cambios en la infraestructura.
- Incrementa la disponibilidad de la red y valida la operación cuando ya la infraestructura esté en funcionamiento.
- Mejora la agilidad de las empresas al establecer estrategias empresariales y tecnológicas.
- Acelera la velocidad de las aplicaciones y servicios al mejorar la disponibilidad; confiabilidad; seguridad; escalabilidad y desempeño general.

VII. RECOMENDACIONES

a) Se sugiere proporcionar formación necesaria a los usuarios para adaptarse al uso de la Red Privada Virtual.

b) Se recomienda implementar y probar el uso de la suite OpenVPN bajo la plataforma de software libre Linux para demostrar la mejora de la seguridad informática en la red de otras empresas.

c) Para garantizar el nivel de satisfacción de los usuarios de Lima Traylers S.A.C., se sugiere crear un manual de usuario para capacitar adecuadamente al personal. Ya que necesitan saber cómo manejar la red privada virtual de manera eficiente.

d) Se propone que esta investigación se use como base para futuras investigaciones similares que puedan ser aplicadas a diferentes empresas y se continúe usando el enfoque de la metodología PPDIOO para la implementación de redes privadas virtuales.

REFERENCIAS

Ales, Ibiza . 2017. *Administracion de redes locales.* francia : s.n., 2017.

Alonso, Luz. 2016. Platzi. [En línea] 26 de Julio de 2016. https://prezi.com/tutrtzgvllkz/flujos-turisticos/.

Atencio, Arturo Ivan y Mamani, Ever Jhonatan. 2017. http://repositorio.unap.edu.pe. [En línea] 03 de 08 de 2017. [Citado el: 14 de 10 de 2020.] http://repositorio.unap.edu.pe/handle/UNAP/5789.

Cadena, Katiusca y Segura, Belén. 2015. *Diseño de una Red Privada Virtual bajo servidores Linux para la carrera dde Ingeniería en Networking y Telecomunicaciones y Análisis de Factibilidad para la Implementación.* Guayaquil : Universidad de Guayaquil Facultad de Ciencias Matemáticas y Físicas Carrera de Ingeniería en Networking y Telecomunicaciones, 2015.

—. 2015. *Diseño de una red privada virtual bajo servidores Linux para la carrera de Ingeniería en Networking y Telecomunicaciones.* Guayaquil : Universidad de Guayaquil, 2015.

Carrillo Flores, Ana Lilia. 2015. uaemex. [En línea] Septiembre de 2015. http://ri.uaemex.mx/oca/view/20.500.11799/35134/1/secme-21544.pdf.

Castillo, José. 2020. https://www.profesionalreview.com. *https://www.profesionalreview.com.* [En línea] 5 de Abril de 2020. [Citado el: 11 de Octubre de 2020.] https://www.profesionalreview.com/2020/04/05/openvpn-que-es/.

Chaves, Pierr y Dueñas, Jorge. 2016. https://es.slideshare.net/. [En línea] 26 de Mayo de 2016. [Citado el: 05 de Noviembre de 2020.] https://es.slideshare.net/PierreAngelo1/prueba-de-normalidad-62410957.

CISCO. 2017. ITESA. [En línea] Instituto Tecnológico Superior del Oriente del Estado de Hidalgo, 2017. [Citado el: 2020 de 11 de 29.] https://www.itesa.edu.mx/netacad/networks/course/module1/1.2.2.1/1.2.2.1.html#:

~:text=El%20modelo%20de%20arquitectura%20empresarial%20de%20Cisco%20separa%20la%20red,y%20la%20resoluci%C3%B3n%20de%20problemas.

Cisco. 2018. Netacad. [En línea] Cisco, 2018. [Citado el: 28 de Octubre de 2020.] https://www.itesa.edu.mx/netacad/networks/course/module1/1.2.2.1/1.2.2.1.html.

Cueva, Araceli. 2018. *Impacto de la implementación de una red privada virtual en la gestión de información de la empresa Deyfor E.I.R.L.* Cajamarca : Universidad Nacional de Cajamarca, 2018.

De La Cruz, Magdaleno y Vera, Jean. 2019. *Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo.* Lambayeque : Universidad Nacional Pedro Ruiz Gallo, 2019.

El Cifrado Web. **Ramírez, Dante y Espinosa, Carmina. 2018.** México : Universidad Nacional Autónoma de México (UNAM), 2018.

Espinoza Chipane, César renato. 2018. *"Propuesta De Una Red Privada Virtual Para Mejorar El Servicio De Comunicación En Las Tiendas Mass Para La Empresa Supermercados Peruanos S.A.".* Lima, Perú : Universidad Autónoma Del Perú, 2018.

Fruhlinger, Josh. 2018. Network World. [En línea] 04 de Julio de 2018. [Citado el: 16 de Octubre de 2020.] https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red.

Garcia Cervigòn, Alfonzo y Alegre Ramos, Maria Del Pilar. 2011. *Seguridad Informatica.* Madrid - España : Ediciones Paraninfa S.A, 2011. 978-84-9732-818-8.

Gomez, Teresa. 2016. *Software libre , software de código abierto, licencias.* París : Universit´e Paris-Est, 2016.

Hernández, Rodrigo, Fernández, Carlos y Baptista, Pilar. 2014. Metodología de la investigación (6ª Edición). [aut. libro] Rodrigo Hernández. *Metodología de la investigación (6ª Edición).* Mexico : Mexico, 2014.

Instituto Nacional de Ciberseguridad. 2017. https://www.incibe.es/. [En línea] 2017. [Citado el: 2020 de 10 de 14.]

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

Instituto Nacional de Estadística e Informática. 2015. *Perú: Tecnologías de Información y Comunicación en las Empresas, 2015.* Lima : s.n., 2015.

Lederkremer, Miguel, [trad.]. 2019. *REDES INFORMATICAS.* BUENOS AIRES - ARGENTINA : s.n., 2019. 978-987-4958-21-1.

Ministerio de Energías y Minas. 2020. http://minem.gob.pe/. [En línea] 2020. [Citado el: 14 de 10 de 2020.] http://minem.gob.pe/_detalle.php?idSector=1&idTitular=159&idMenu=sub149&idCateg=159.

Network, Palo Alto. 2020. https://www.paloaltonetworks.com/. [En línea] Palo Alto Network, 2020. https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn.

networkworld. 2018. https://www.networkworld.es/. [En línea] 04 de 07 de 2018.

Pomar, Rafael. 2019. *Implementacion de una red privada virtual de software libre en una empresa.* España : Universidad Abierta de Cataluña, 2019.

Postigo Palacios, Antonio. 2020. *Seguridad Informatica.* Madrid - España : Ediciones Paraninfo S.A, 2020. 9787-84-283-4455-5.

Prieto Cristancho, Yudy Yohanna. 2011. https://gunilibre.edu.co. [En línea] 14 de Agosto de 2011. https://repository.unilibre.edu.co/bitstream/handle/10901/8838/IMPLEMENTACION%20DE%20L%20RED%20PRIVADA%20VIRTUAL%20%28VPN%29%20A%20LAS%20SUCURSALES%20Y%20USUARIOS%20EXTERNOS%20DE%20LA%20EMPRESA.pdf?sequence=1&isAllowed=y.

QUIDAN. 2020. *METODOLOGÍA PPDIOO.* UNIVERSIDAD DE GUAYAQUIL - ECUADOR : s.n., 2020.

Ramírez Páez, Luis Ernesto. 2018. https://usta.edu.co. [En línea] 2018. https://repository.usta.edu.co/bitstream/handle/11634/14804/2019luisramirez.pdf?sequence=4&isAllowed=y.

Ramirez Varone, Martin Orlando. 2020. *Rendimiento de una red utilizando vlans como propuesta de diseño en el E.S. II-1 Hospital Chulucanas Manuel Javier Nomberto.* Piura : Universidad César Vallejo, 2020.

Romero Castro, Martha Irene y Figueroa Moran, Grace Liliana . 2018. *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicante - España : ÁREA DE INNOVACIÓN Y DESARROLLO, S.L, 2018.

Salazar, Diego Alfredo. 2017. *La gestion del tiempo como factor clave en las habilidades directivas aplicadas al sector turistico.* Ecuador : Escuela Universitaria de Turismo, Universidad de Murcia, 2017. 2172-8690.

Sanchez, Alvaro. 2018. *Implementación de una VPN en una red corporativa para mejorar la gestión de la información de los servicios en la empresa Técnica Plástica SRL.* Lima : Repositorio Universidad César Vallejo, 2018.

SearchData. 2016. https://searchdatacenter.techtarget.com/es. [En línea] 2016. [Citado el: 17 de 10 de 2020.] https://searchdatacenter.techtarget.com/es/definicion/Red-privada-virtual-VPN.

ServisoftCorp. 2019. ServisoftCorp. [En línea] 19 de Febrero de 2019. https://www.servisoftcorp.com/definicion-y-como-funcionan-las-aplicaciones-moviles/.

Simpson, Scott. 2019. *Learning VPN.* s.l. : linkedin.com, 2019.

Sivasubramanian, Balaji, Frahim, Erum y Froom, Richard. 2010. https://www.ciscopress.com. [En línea] 15 de Julio de 2010. [Citado el: 11 de Octubre de 2020.] https://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3.

Student's t. Uses and abuses. **Sánchez, Reinaldo. 2015.** 1, México : Revista mexicana de cardiología, 2015, Vol. 26. ISSN 0188-2198.

Tacilla Ludeña, JULIO LUIS. 2016. *SISTEMA INFORMÁTICO WEB DE GESTIÓN DE INCIDENCIAS.* Trujillo : Universidad Privada Antenor Orrego, 2016.

Valencia, Universidad Internacional de. 2020. https://www.universidadviu.com/. [En línea] 2020. https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme.

VERA NAVARRETE, DENISSE. 2018. *INTRODUCCION A LA SEGURIDAD INFORMATICA Y EL ANALISIS DE VULNERABILIDAD.* ALICANTE - ESPAÑA : s.n., 2018. 978-84-949306-1-4.

Yonan, James. 2018. Open Vpn. [En línea] 2018. [Citado el: 03 de Octubre de 2020.] https://openvpn.net/.

ANEXOS

Tabla 31. Matriz de Consistencia

Título: Implementación de una Red Privada Virtual basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C.

MATRIZ DE CONSISTENCIA				
PROBLEMA GENERAL	**OBJETIVOS**	**HIPÓTESIS GENERAL**	**VARIABLES**	**METODOLOGÍA**
¿De qué manera el uso de una red privada virtual, basada en la metodología PPDIOO, mejora la seguridad informática en la red de la empresa Lima Traylers SAC?	Mejorar la seguridad informática de la red en la empresa Lima Traylers S.A.C, mediante la implementación de una red privada virtual basada en la metodología PPDIOO.	La implementación de una red virtual privada basada en la metodología PPDIOO mejora significativamente la seguridad informática en la red de Lima Traylers S.A.C.	**Variable Independiente:** Red Privada Virtual **Variable Dependiente:** Seguridad informática en la red de la empresa Lima Traylers SAC **Indicadores:** * Cantidad de incidencias reportadas por los usuarios. * Cantidad de usuarios conectados en la red. * Tiempo para acceder a las carpetas compartidas. Nivel de satisfacción de los usuarios.	**Tipo de investigación:** Aplicada **Nivel de investigación:** Experimental puro **Tecnica de investigacion:** Observacion directa Observacion indirecta **Población - Universo:** Población: Todos los procesos de la seguridad informática de la red en micro y pequeñas empresas de carrocerías para tráilers. N= Indeterminado **Muestra:** Procesos de la seguridad informática de la red en la empresa Lima Traylers S.A.C. n = 30

Tabla 32. Reporte de Incidencias

Reporte de Incidencias Lima Traylers				
Ticket	Descripsion	Estado	Prioridad	fecha
1300	Correo no envia (Archivo muy pesado)	Cerrado	Alta	1/01/2021
1301	No puedo conpartir informacion	cerrado	Alta	1/01/2021
1302	Demora mucho tiempo en cargar imágenes	cerrado	Alta	1/01/2021
1303	No tengo acceso a las camaras	cerrado	Alta	2/01/2021
1304	Correo no descarga (archivo sospechoso)	cerrado	Alta	2/01/2021
1305	Impresora no escanea	cerrado	Alta	3/01/2021
1306	No tengo acceso a carpeta compartida	cerrado	Alta	3/01/2021
1307	Correo no envia (Archivo muy pesado)	cerrado	Alta	4/01/2021
1308	Falla de impresión en impresora ingenieria	cerrado	Alta	5/01/2021
1309	Sin acceso a internet	cerrado	Alta	5/01/2021
1310	inconveniente en data transfer	cerrado	Alta	5/01/2021
1311	Camaras inoperativas	cerrado	Alta	5/01/2021
1312	Problemas al realizar imprimir factura	cerrado	Alta	6/01/2021
1313	No puedo enviar factura a contabilidad	cerrado	Alta	6/01/2021
1314	Correo no descarga (archivo sospechoso)	cerrado	Alta	6/01/2021
1315	Correo me rebota	cerrado	Alta	7/01/2021
1316	Erreor de imprecion en de guia (Nro PEDIDO 2102001162)	cerrado	Alta	8/01/2021
1317	No puedo ingresar a la carpeta compartida desde la nube de mi area	cerrado	Alta	8/01/2021
1318	No puedo ver camara de planta chacracerro	cerrado	Alta	9/01/2021
1319	CORREOS COLGADOS Y CARPETA COMPARTIDA ERROR	cerrado	Alta	9/01/2021
1320	ONEDRIVE: LAS CARPETAS DE IMPORTACIONES DE 2020 SE ENCUENTRAN VACIAS	cerrado	Alta	9/01/2021
1321	Problema de transferencia	cerrado	Alta	10/01/2021
1322	no hay wathsap	cerrado	Alta	10/01/2021
1323	Archivos no se pueden abrir	cerrado	Alta	10/01/2021
1324	Acceso a carpeta compartida	cerrado	Alta	11/01/2021
1325	no se puede descarga la carpeta fotos mantto	cerrado	Alta	11/01/2021
1326	compresor 3 no se puede abrir archvio	cerrado	Alta	11/01/2021
1327	ACTUALIZACIÓN WINDOWS	cerrado	Alta	11/01/2021
1328	Falla de impresión en impresora ingenieria	cerrado	Alta	12/01/2021
1329	No puedo conpartir informacion	cerrado	Alta	12/01/2021

Tabla 33. Comparativo de Protocolos VPN

CUADRO COMPARATIVO DE PROTOCOLOS VPN					
	PPTP	L2TP	OpenVpn	SSTP	IKEV2
VENTAJAS	✓ Rápido. ✓ Cliente incorporado en casi todas las plataformas. ✓ Fácil de configurar.	✓ Generalmente considerado seguro. ✓ Disponible en todos los dispositivos y sistemas operativos modernos. ✓ Fácil de configurar	✓ Tiene la habilidad de superar la mayoría de los cortafuegos ✓ Muchas opciones de configuración ✓ Como es de código abierto, se puede investigar fácilmente cualquier ingreso clandestino ✓ Es compatible con varios algoritmos de codificación ✓ Muy seguro	✓ Tiene la capacidad de superar la mayoría de los cortafuegos ✓ El nivel de seguridad depende del cifrado, pero generalmente es seguro. ✓ Totalmente integrado en el sistema operativo Windows ✓ Soporte de Microsoft	✓ Extremadamente seguro. Soporta una variedad de cifrados como 3DES, AES, AES 256. ✓ Viene con soporte para dispositivos BlackBerry ✓ Es estable, especialmente al reconectarse después de perder la conexión o cambiar de red ✓ Es fácil de configurar, al menos desde el lado del usuario ✓ Relativamente más rápido que L2TP, PPTP y SSTP.
DESVENTAJAS	✓ Está en peligro frente a la NSA ✓ No es completamente seguro	✓ Más lento que OpenVPN. ✓ Puede estar en riesgo frente a la NSA. ✓ Puede ser problemático si se usa con cortafuegos restrictivos. ✓ Es probable que la NSA haya debilitado el	✓ Requiere programas de terceros ✓ El soporte para computadoras de escritorio es genial, pero necesita mejoras para los dispositivos móviles	✓ Como es una estándar propiedad de la Corporación Microsoft, no puede ser analizado en busca de ingresos clandestinos ✓ Solo funciona en plataformas Windows	✓ Compatible con plataformas limitadas ✓ El puerto UDP 500 utilizado es fácil de bloquear en comparación con las soluciones basadas en SSL, como SSTP u OpenVPN ✓ No tiene implementación de código abierto ✓ En el lado del servidor, implementar IKEv2 es dificultoso, lo cual puede causar algunos problemas potenciales